



TRABAJO FIN DE GRADO

GRADO EN DERECHO

CURSO ACADÉMICO 2016-2017

**LA PROTECCIÓN DE DATOS PERSONALES POR EL TRIBUNAL
EUROPEO DE DERECHOS HUMANOS Y LA INCIDENCIA DE LA
TECNOLOGÍA EN SU EVOLUCIÓN**

**PROTECTION OF PERSONAL DATA BY THE EUROPEAN
COURT OF HUMAN RIGHTS AND THE INCIDENCE OF
TECHNOLOGY ON ITS EVOLUTION**

AUTORA: Lidia Boza Díaz

DIRECTORA: Yaelle Cacho Sánchez

Resumen

El Tribunal Europeo de Derechos Humanos es uno de los órganos internacionales de referencia para estudiar la protección de los derechos humanos y libertades fundamentales de las personas, y entre ellos, el derecho a la protección de los datos personales. Sin embargo, el Tribunal no concibe este derecho como un derecho humano autónomo, sino que lo incardina en el derecho al respeto de la vida privada y familiar. El reconocimiento jurisprudencial de esta área de protección ha sido muy tardío, y cabe apreciar cómo durante la formación de este concepto y en su desarrollo posterior, la tecnología ha tenido un papel determinante e insustituible.

No obstante, la protección del Tribunal en la actualidad es, cuanto menos, poco satisfactoria. Y ello se debe principalmente a que la regulación nacional e internacional atiende al carácter económico de la información, y presta poca atención a las garantías del individuo. Este factor tiene como principal aliado al nuevo desarrollo tecnológico, que es su principal herramienta para perpetrar las injerencias en la privacidad de las personas. Así, la lucha contra estos fuertes elementos es difícil de atajar por el TEDH, realmente limitado por la carta de derechos que protege y por las concepciones de los Estados en la materia.

Abstract

The European Court of Human Rights is one of the international reference bodies for studying the protection of human rights and fundamental freedoms of individuals, including the right to the protection of personal data. However, the Court does not conceive of this right as an autonomous human right, but includes it in the right to respect for private and family life. The jurisprudential recognition of this area of protection has been very late. In addition, during the formation of this concept and in its later development, technology has had a decisive and irreplaceable role.

However, the protection of the Court at present is, at the very least, unsatisfactory. And this is mainly due to the fact that national and international regulation is characterized by the economic nature of the information, and gives little attention to the guarantees of the

individual. This factor has as main ally to the new technological development, which is its main tool to perpetrate the interference in the privacy of people. Thus, the fight against these strong elements is difficult to tackle by the ECtHR, which is actually limited by the charter of rights it protects and by the conceptions of States in the matter.

I. INTRODUCCIÓN

II. LA PROTECCIÓN DE DATOS PERSONALES

2.1. ORIGEN.....	13
2.2. RECONOCIMIENTO Y DESARROLLO EN EL PLANO NACIONAL.....	14
2.3. NECESARIA APROXIMACIÓN INTERNACIONAL.....	18
2.4. DEFINICIÓN DEL CONCEPTO.....	20

III. LA PROTECCIÓN DE DATOS PERSONALES EN EL SENO DEL CONSEJO DE EUROPA

3.1. UN RECORRIDO HISTÓRICO.....	25
3.2. EL CONVENIO 108 PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL (1981):	31
3.2.1. Forma.....	32
3.2.2. Contenido.....	34
3.3. PROTOCOLO ADICIONAL AL CONVENIO 108 (2001).....	38
3.4. MODERNIZACIÓN DEL CONVENIO 108 (2017).....	41

IV. LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES: ANTECEDENTES

4.1. INTRODUCCIÓN.....	45
4.2. ANTECEDENTES DE LA PROTECCIÓN DE DATOS PERSONALES: LA JURISPRUDENCIA SOBRE EL DERECHO AL RESPETO A LA VIDA PRIVADA Y FAMILIAR, DOMICILIO Y CORRESPONDENCIA (ART. 8 CEDH) DURANTE EL S. XX (DE 1978 A 1997).....	49
4.2.1. Tratamiento general: contenido del derecho y principios.....	49
4.2.2. Relación con otros derechos.....	52
4.2.3. Acciones de las personas.....	53
4.2.4. Obligaciones de los Estados.....	54

V. LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES: RECONOCIMIENTO Y DESARROLLO

5.1. RECONOCIMIENTO DE LA PROTECCIÓN DE DATOS PERSONALES: CASO Z. c. FINLANDIA, DE 1997.....	57
5.2. DESARROLLO DE LA PROTECCIÓN DE DATOS PERSONALES: LA JURISPRUDENCIA SOBRE EL DERECHO AL RESPETO A LA VIDA PRIVADA Y FAMILIAR, DOMICILIO Y CORRESPONDENCIA (ART. 8 CEDH) DURANTE EL S. XXI (DE 1997 A 2017).....	59
5.2.1. Tratamiento general: contenido del derecho y principios.....	59
5.2.2. Relación con otros derechos.....	63
5.2.3. Acciones de las personas.....	66
5.2.4. Obligaciones de los Estados.....	69
5.3. EVOLUCIÓN: LA INCIDENCIA DE LA TECNOLOGÍA DEL S. XXI EN LA JURISPRUDENCIA DEL TEDH	71
5.3.1. Internet, principal herramienta de interceptación de las comunicaciones.....	71

5.3.2. Recogida de muestras de ADN relacionadas con la justicia penal.....	73
5.3.3. Técnicas de localización geográfica.....	74
5.3.4. Almacenamiento informático de datos personales y sus nuevos tratamientos: decisiones maquinizadas y acercamiento al Big Data.....	74

VI. CONSIDERACIONES FINALES

BIBLIOGRAFÍA

ANEXOS

**Anexo 1. La Jurisprudencia del TEDH en materia de protección de datos:
datos generales**

**Anexo 2. La Jurisprudencia del TEDH en materia de protección de datos:
orden cronológico**

**Anexo 3. La Jurisprudencia del TEDH en materia de protección de datos:
datos cualitativos y cuantitativos por décadas**

**Anexo 4. La Jurisprudencia del TEDH en materia de protección de datos:
contenido del derecho**

**Anexo 5. La Jurisprudencia del TEDH en materia de protección de datos:
principios en el tratamiento del derecho por parte del Tribunal**

**Anexo 6. La Jurisprudencia del TEDH en materia de protección de datos:
derechos en conflicto con el derecho a la protección de datos personales**

**Anexo 7. La Jurisprudencia del TEDH en materia de protección de datos:
acciones de las personas**

**Anexo 8. La Jurisprudencia del TEDH en materia de protección de datos:
obligaciones de los Estados**

**Anexo 9. La Jurisprudencia del TEDH en materia de protección de datos:
reconocimiento expreso de la protección de datos personales por parte el
TEDH y su relación con el Convenio 108**

**Anexo 10. La Jurisprudencia del TEDH en materia de protección de datos:
casos con mayor incidencia de las nuevas tecnologías**

ÍNDICE DE ABREVIATURAS

Convenio 108	Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal
Protocolo Adicional	Protocolo Adicional al Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal
Modernización del Convenio	Borrador sobre la modernización del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal
C.d.E.	Consejo de Europa
T.E.D.H.	Tribunal Europeo de Derechos Humanos
T.C.A.	Tribunal Constitucional Alemán
C.E.D.H.	Convenio Europeo de Derechos Humanos
O.E.A.	Organización de los Estados Americanos
O.C.D.E.	Organización para la Cooperación y el Desarrollo Económicos
U.E.	Unión Europea
T.F.U.E.	Tratado de Funcionamiento de la Unión Europea
S.	Siglo

I. INTRODUCCIÓN

La necesidad de regular la protección de datos personales no es un fenómeno novedoso. Hunde sus raíces en los últimos años del s. XIX, tal y como recuerdan la mayoría de las obras consultadas, que se verán en capítulos posteriores de este trabajo. Sin embargo, los avances tecnológicos que se han producido desde entonces, han hecho necesario que la respuesta dada por el Derecho evolucionara. Esta necesidad se ha dejado sentir especialmente con la problemática que se expone a continuación.

El punto de inflexión a la hora de enfrentar la protección de datos personales lo constituye la transición tecnológica que ha habido desde finales del s. XX a inicios del s. XXI, y el crecimiento exponencial que ha experimentado hasta la actualidad. El avance tecnológico supuso desde finales del pasado siglo, un giro copernicano que comenzó a afectar a todos los sectores de la sociedad. Desde entonces, el acceso a la información empezó a ser cada vez más sencillo, y a superar progresivamente fronteras en el tiempo y en el espacio. Ello ha supuesto la evolución de la sociedad, y nuevos estilos de vida que pueden apreciarse hoy simplemente observando las diferencias entre las generaciones propias del s. XX y s. XXI que coexisten en la actualidad. En este sentido, internet y la era digital han jugado un papel esencial. La ingente cantidad de información vertida en la red comenzó a necesitar de un procesamiento de datos que, a medida que la tecnología aumentaba, su desarrollo y capacidad también. Ello supuso el paso de una administración de datos centralizada a descentralizada, dejando atrás los enormes bancos de datos a la miniaturización de los procesadores¹.

Todo el nuevo desarrollo de la tecnología durante este periodo de tiempo nos lleva directamente al concepto de Big Data. El Big Data representa un nuevo paradigma en la manera en que la información es recopilada, combinada y analizada. Supone una nueva interacción entre entornos tecnológicos, entre ellos Internet y la computación en nube. Puede llegar a ser una innovación significativa para la sociedad, pero a la vez, el Big Data permite recopilar y analizar grandes cantidades de datos para identificar patrones de actitud y predecir comportamientos de grupos y comunidades, y cada vez más también

¹ CHIRINIO SÁNCHEZ, A., "Autodeterminación informativa y Estado de Derecho en la sociedad tecnológica", CONAMAJ, San José, 1997, p.23. Disponible en <http://ocw.uned.ac.cr/eduCommons/s.e.p/tecnologia-y-trabajo/tutorias/tutoria-segunda/autodeterminacion-informativa-y-estado-de-derecho-en-la-sociedad-tecnologica-alfredo-chirino/view>. Consultado el 1 de mayo de 2017

de individuos, de manera que cabe considerar los riesgos que van relacionados con el uso de esos datos².

¿Cómo se ha llegado al Big Data? La navegación por internet no es en ningún caso oculta, y el uso de la tecnología (*smartphones*, sus aplicaciones, etc.), como todo usuario sabe, normalmente requiere la identificación de la persona como mínimo paso inicial. De esta manera, muchísimos datos personales pueden ser recolectados por el paso del usuario en la red, desde datos meramente identificativos de la persona, a datos que, como se verá más adelante, tienen la característica de “sensibles”. Es decir, aquellos que, por afectar al reducto más íntimo de la personalidad, requieren una garantía más fuerte. Son, los que se refieren a las creencias religiosas, filosóficas o ideológicas, los que afectan al origen racial, la sexualidad o a la salud³. Datos que puedan de alguna manera hacer referencia a la personalidad. Y todos ellos son altamente fáciles de controlar. Muchas veces, simplemente aceptando al uso de ciertas páginas web o ciertas aplicaciones, se está dando el consentimiento a la recolección de esos datos sensibles para su procesamiento con diversos fines, incluso a su traspaso transfronterizo para su venta. Éste último aspecto es un tema de absoluta actualidad: el crecimiento de los flujos internacionales de datos de carácter personal entre las filiales de una empresa multinacional, utilización de herramientas multiacceso, prestación de servicios desde distintos países, en áreas tales como la de los recursos humanos, los servicios financieros, la banca, la educación, el comercio electrónico, el auxilio judicial internacional o la investigación en el área de la salud; que son ahora una parte integral de la economía globalizada⁴.

Bien es cierto que, parafraseando a Chirino⁵, el intercambio de informaciones, la comparación de datos, la conformación de perfiles de personalidad son actividades no sólo tecnológicamente posibles, sino también necesarias para la sociedad de mercado en la que estamos viviendo. Además, toda esta información es necesaria para la toma de decisiones, tanto para la administración pública como para el sector privado. Cabe destacar que, mientras que durante el s. XX la protección de datos personales, como mucho, podría suponer una pugna o ponderación de derechos o intereses; desde la

² COUNCIL OF EUROPE, T-PD(2017)01, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasbourg, 2017, p. 1. Disponible en <https://rm.coe.int/16806ebe7a>. Consultado el 1 de mayo de 2017.

³ MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 4

⁴ ORTEGA JIMÉNEZ, A., *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, Tesis doctoral, Alicante, 5 de septiembre de 2014

⁵ CHIRINIO SÁNCHEZ, A., *op. cit.*, p.26.

revolución tecnológica a inicios del s. XXI, la protección de datos se enfrenta al valor económico de la información⁶, en manos del sector privado prácticamente en su totalidad. Este marcado carácter económico de la información, puede ser el aspecto más característico de la protección de datos en este momento de la historia, y el reto más difícil a la hora de abordar su regulación y su protección por el Derecho.

Otro peligro al que nos enfrentamos ante el procesamiento es, no tanto el valor económico que se le pueda dar a la información, sino la idea de tendencia actual de necesitar más seguridad restringiendo nuestra libertad, que en un futuro próximo pueda llegar hasta límites insospechados. Como dice CHIRINO,

“Si el ciudadano no tiene posibilidad de controlar quién tiene acceso a sus datos, con qué objetivos, y bajo qué presupuestos, pronto tendrá que desistir al ejercicio de sus derechos fundamentales, ya que muchas libertades públicas (como la libertad de asociación y de reunión, así como las libertades de expresión y autodeterminación), se convertirán en meras formas sin contenido, ya que aumentarían al mismo tiempo las posibilidades a fin de impedir o al menos amedrentar a quienes deseen ejercer tales libertades, no con prohibiciones directas, sino con la aplicación de consecuencias indirectas al mero ejercicio de un derecho”⁷.

Frente a esta situación existen diversas corrientes a la hora de valorar el fenómeno de Internet y la tecnología que está invadiendo nuestra sociedad. Los *apocalípticos*, aquellos que desconfían de la red, por ver en ella un riesgo de debilitamiento del *status* de ciudadanía y los valores de la democracia, suplantados por la lógica económica del mercado y dando lugar a la identificación del ciudadano con el consumidor pasivo de los programas producidos por los grandes poderes económicos. Por otra parte, la visión *de los integrados*, que tiende a hablar de la *ciberciudadanía* o del hombre cibernético y acaba presentando a la sociedad internauta como la sociedad madura⁸.

⁶MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 58

PIÑAR MAÑAS, J.L., *El Derecho a la autodeterminación informativa: Protección de datos: origen, situación actual y retos de futuro*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p.92

⁷ CHIRINIO SÁNCHEZ, A., *op.cit.*, p.31

⁸ RODRIGUEZ PALOP, M.A., “PÉREZ LUÑO, A.E., La tercera generación de derechos humanos, *Aranzadi*, Navarra, 2006, 315 pp.”, *Derechos y Libertades*, Número 16, Época II, enero 2007, pp. 277-284, p.280

Toda esta problemática que genera la era digital es de interés no sólo por el fenómeno como tal, sino también por la respuesta que está intentando darse por parte del Derecho. Se han adoptado diferentes instrumentos normativos tanto en el plano nacional como en el internacional, aunque a efectos de este trabajo ha llamado especialmente la atención esta última vertiente, por su estrecha conexión con la protección internacional de los derechos humanos. Especialmente llamativa ha resultado la labor llevada a cabo en este ámbito por el Consejo de Europa (en adelante, CdE), y en particular, la protección otorgada a los datos personales por uno de los órganos creados en su seno, el Tribunal Europeo de Derechos Humanos (en adelante, TEDH). Este interés viene acrecentado, si cabe, por el hecho de que desde la adopción del *Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales* (en 1950), sobre la base de los fundamentos ideológicos de promoción y protección de los derechos humanos⁹, el Consejo de Europa ha desarrollado una gran función, tanto codificadora como de protección, que permite concluir que “la defensa de los derechos humanos constituye en la actualidad una de las actividades centrales de esta Organización, lo que la convierte en la punta de lanza del proceso global de protección de los derechos humanos en Europa”¹⁰.

Por todo ello, se decidió que el objeto de este trabajo fuera el estudio de la protección de datos personales por el Tribunal Europeo de Derechos Humanos, teniendo en cuenta la especial incidencia de la tecnología. Como puede observarse, los objetivos son fundamentalmente dos: el primero, el posicionamiento del TEDH respecto a la protección de los datos personales, y el segundo, la incidencia de la tecnología en la tutela ofrecida por el Tribunal. Sin embargo, para dar respuesta a estos dos interrogantes, se ha requerido de una contextualización previa, tanto en el plano general como en el marco del Consejo de Europa, debido a la cantidad de factores que han influido en la formulación de esta materia en la jurisprudencia del Tribunal.

Así, en el segundo capítulo, se hace referencia a esta necesaria contextualización general de la protección de los datos personales. De esta manera, se hace referencia a su origen, a cómo los distintos Estados han reconocido esta área de protección y han abordado la

⁹ Art. 3 Estatuto del Consejo de Europa: “Cada uno de los Miembros del Consejo de Europa reconoce el principio del imperio del Derecho y el principio en virtud del cual cualquier persona que se halle bajo su Jurisdicción ha de gozar de los derechos humanos y de las libertades fundamentales, y se compromete a colaborar sincera y activamente en la consecución de la finalidad definida en el capítulo primero”.

¹⁰ DIEZ DE VELASCO VALLEJO, M., “Capítulo XXVIII. La protección internacional de los derechos humanos (II)”, en DIEZ DE VELASCO VALLEJO, M., *Instituciones de Derecho Internacional Público*, 18ª Edición, Tecnos, Madrid, 2013, pp. 698-699.

regulación de la materia; cómo diversas organizaciones internacionales también han mostrado interés por ello, y, finalmente, se ofrecerán algunos intentos de definición de la materia por parte de la doctrina.

El tercer capítulo tratará, por lo tanto, de los factores y antecedentes que, dentro del seno del Consejo de Europa, han influido en la formación jurisprudencial de la protección de datos personales por parte del TEDH. De esta manera, se expondrá en primer lugar un recorrido histórico, comenzando por el necesario punto de partida del Tribunal en el derecho al respeto a la vida privada y familiar, domicilio y correspondencia; consagrando en el art. 8 del Convenio Europeo de Derechos Humanos de 1950. En segundo lugar, se abordará cómo ha ido evolucionando las labores de protección de la materia por parte del Consejo de Ministros, hasta llegar a la elaboración del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (en adelante, Convenio 108), y su Protocolo Adicional. Y, en tercer lugar, se explicará la modernización de dicho Convenio, que está teniendo lugar desde 2010. Todo este recorrido histórico se explicará porque, como se verá en el capítulo IV, tiene una incidencia directa en la jurisprudencia del Tribunal. En este sentido, durante todo este desarrollo explicativo, se apreciará brevemente el desarrollo paralelo que la jurisprudencia del T.E.D.H. ha ido elaborando, a medida que el resto de órganos del Consejo de Europa iban estableciendo otros mecanismos de protección.

Los capítulos cuarto y quinto, por fin procederán a abordar la jurisprudencia del TEDH mediante un método de análisis empírico-analítico. Así, el capítulo cuarto, tratará especialmente de la jurisprudencia que se constituye como antecedente del reconocimiento expreso de la protección de datos personales por parte del Tribunal. Es decir, de la jurisprudencia sobre el art. 8 CEDH durante el s. XX, entre los años 1978 a 1997; caracterizada por la incidencia de la tecnología propia de la sociedad de la información. Y el quinto capítulo, tratará de la jurisprudencia que reconoce la protección de los datos personales y que desarrolla su tutela. Es decir, de la jurisprudencia sobre el art. 8 CEDH durante el s. XXI, entre los años 1997 a 2017; caracterizada por la incidencia de la tecnología propia de la era digital. Finalmente, este capítulo se cerrará con el análisis de la incidencia real de la tecnología más puntera del s. XXI sobre la protección de datos personales por el TEDH. El presente finalizará con unas consideraciones finales sobre todos los resultados obtenidos en la investigación.

II. LA PROTECCIÓN DE DATOS PERSONALES

2.1. ORIGEN

Son varios los autores¹¹ que coinciden en que el antecedente más remoto de la protección de datos es el derecho a la intimidad, siendo la obra *The Right to Privacy*, por Warren y Brandeis, publicada en 1890¹² el primer paso hacia el mismo. Los autores de esta obra partieron del “right to be let alone” formulado por el juez Cooley¹³. Básicamente defendían una intimidad que estaba mayormente vinculada con la prensa, en cuanto a las posibilidades que ésta tenía para obtener información de la vida privada de personas de cierta clase social. Es necesario destacar cómo este primer origen responde en gran medida a los nuevos dispositivos tecnológicos creados como consecuencia de la Revolución Industrial, que el nuevo periodismo social podía utilizar de cara a sus objetivos (las instantáneas fotográficas, la perfección de la imprenta, la radio, etc.) En resumen, podría decirse que es un derecho a ser “dejado solo” o “ser dejado en paz”.

Un segundo antecedente de la protección de datos personales ha sido la defensa del concepto estadounidense *privacy* (traducido como privacidad o vida privada) en lugar de la intimidad, por considerar que es más amplio que ésta¹⁴, y así, se constituye como una mejor base para el futuro desarrollo de la protección de datos¹⁵. Ello ha llevado a autores

¹¹ Entre otros: MARTÍNEZ MARTINEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Colección “protección de datos”, THOMSON CIVITAS, 2004, p.41, 68,69; MURILLO DE LA CUEVA, P.L., “El derecho a la autodeterminación informativa y la protección de datos personales”, *Azpilcueta*, N.º 20, 2008, p.45; SALTOR, C.E., *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina*, Tesis doctoral, Madrid, 2013, p.29,31,32; PIÑAR MAÑAS, J.L., *El Derecho a la autodeterminación informativa: Protección de datos: origen, situación actual y retos de futuro*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p.83; MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p.70

¹² WARREN S. D., BRANDEIS L.D., *El derecho a la intimidad*, (traducción de Benigno Pendás y Pilar Baselga del original “The right to privacy”, *Harvard Law Review*, 1890). Civitas, Madrid, 1996.

¹³ COOLEY, T.M.: *A treatise on the Law of Torts*. Callaghan & Company, Chicago, 1888, en nota n.º 21, de *Op. cit.*, MARTÍNEZ MARTINEZ, R., p. 69.

¹⁴ MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p.7

¹⁵ Mientras que la intimidad puede definirse como la zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia (RAE), o como el derecho del individuo a decidir por sí en qué medida o en qué circunstancias desea compartir con terceras personas sus pensamientos, sentimientos y expresiones personales (Herrán Ortiz, A. La violación de la intimidad en la protección de datos personales. Editorial Dykinson, Madrid, 1998, p.2.); la privacidad, es mucho más amplia que el mero poder de exclusión del conocimiento de los demás de la esfera personal: abarca desde la mera tutela del domicilio y en general la esfera inmaterial de la persona en todo lo que desea tener reservado, hasta la misma propiedad privada, la facultad de guardar silencio sobre opiniones, actividades, afiliaciones políticas propias o de otros, el derecho de las asociaciones a no comunicar el elenco de sus miembros e incluso una tutela de tipo instrumental. Se afirma, en efecto, que la persona que sabe que sus opiniones o comportamientos van a ser conocidos o investigados, se encontrará coartada a para llevarlos a la práctica. ORTI VALLEJO, A., “El nuevo derecho fundamental (y de la personalidad) a la libertad informática”, *Derecho Privado y Constitución*, Núm. 2, enero-Abril 1994, p.8;

y juristas norteamericanos¹⁶ como WESTIN, FRIED o MILLER, a que introdujeran una nueva acepción de la *privacy*, “*informational privacy*”, que se define como “el atentado a la persona perpetrado por la simple recogida y catalogación de informaciones, nueva modalidad que se une al concepto tradicional de *privacy of disclosure*, en el que se engloban los atentados provocados por la difusión y revelación de noticias y datos personales cuyo conocimiento está limitado a un círculo restringido”¹⁷. Esta nueva aproximación se debe también, en gran parte, al contexto tecnológico. Alrededor de los años 60, aparece la sociedad de la información¹⁸. Esta sociedad toma conciencia del valor de la información para el desarrollo, y trata de utilizarla en todos los aspectos de la vida para hacerla más eficiente y productiva. La información supondrá una mejora del sistema político y de la democracia, y una forma de permitir al hombre ocuparse en cuestiones más relacionadas con el intelecto y el espíritu. En este sentido, la información adquiere valor cuando se concibe para ser usada en esos fines, y así, se hace uso de la tecnología de la época para poder sacar un mejor provecho, superando el telégrafo y el teléfono, y llegando a medios como la radio y la televisión. De esta manera, puede apreciarse que esta etapa se caracteriza principalmente por una cuestión de ponderación de derechos, para una convivencia pacífica en las sociedades democráticas.

2.2. RECONOCIMIENTO Y DESARROLLO EN EL PLANO NACIONAL

Puede apreciarse, por lo tanto, un consenso generalizado sobre los antecedentes de la protección de datos personales. Pero en lo que respecta al reconocimiento y desarrollo de la materia en América y Europa, adoptará caminos divergentes, como se verá a continuación.

Por lo que se refiere a América Central y América del Sur, el desarrollo de la protección de datos tiene su máximo exponente en la introducción de una facultad de acceso a los

SALTOR, C.E., *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina*, Tesis doctoral, Madrid, 2013, p.34

¹⁶ Para más información, véase MARTÍNEZ MARTINEZ, R., *Una aproximación crítica a la autodeterminación informativa*, THOMSON CIVITAS, 2004, Estudios de Protección de datos, p. 78-102, y notas 54 y 59

¹⁷ MARTÍNEZ MARTINEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Colección “Protección de datos”, THOMSON CIVITAS, 2004, p. 78; ORTI VALLEJO, A., “El nuevo derecho fundamental (y de la personalidad) a la libertad informática”, *Derecho Privado y Constitución*, Núm. 2, enero-abril 1994, p.312

¹⁸ Para ver descripción del término “sociedad de la información”, ver CHIRINIO SÁNCHEZ, A., “Autodeterminación informativa y Estado de Derecho en la sociedad tecnológica”, CONAMAJ, San José, 1997, nota 5. Disponible en <http://ocw.uned.ac.cr/eduCommons/s.e.p/tecnologia-y-trabajo/tutorias/tutoria-segunda/autodeterminacion-informativa-y-estado-de-derecho-en-la-sociedad-tecnologica-alfredo-chirino/view>. Consultado el 1 de mayo de 2017

datos personales en las constituciones. Es el *habeas data*, incorporado en casi todas las constituciones de los Estados de la región a partir de 1980, siendo Brasil la primera en incorporarlo en la reforma Constitucional de 1985. Una vez introducida esta disposición constitucional, se adoptarán en general las leyes de protección de datos personales, por influencia del derecho comparado europeo¹⁹. Esta garantía del *habeas data*, en resumen, constituye un cauce procesal constitucional al derecho a la autodeterminación informativa, para proteger los datos personales y la libertad de la persona ante la acumulación y procesamiento informático de sus datos personales. Así, se garantiza al afectado el ejercicio de su facultad de solicitar información sobre su persona, y ejercer un efectivo control sobre ella. La acción de *habeas data* se define como:

“el derecho que asiste a toda persona -identificada o identificable- a solicitar judicialmente la exhibición de los registros -públicos o privados- en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación. Constituye, en suma, una acción procesal concreta, expedita y rápida, que toma la forma de una especie de amparo, para salvaguardar la libertad de la persona ante la acumulación y procesamiento informático de sus datos personales”²⁰.

En Estados Unidos, ya en 1973 el Departamento de Salud, Educación y Bienestar propuso un Código de buenas prácticas que recogería los principios que habrían de regir el uso de información por parte del Gobierno (*Fair Information Practices o Fair Information Principle*). En 1974, se aprueba la *Privacy Act* de Estados Unidos, y van asentándose las bases de los principios esenciales que configuran del derecho a la privacidad²¹. Estados Unidos ha optado por una legislación de tipo sectorial, con protección en áreas específicas, que necesitan de una regulación para proteger a las personas de los efectos perjudiciales que pueda tener el tratamiento automatizado de sus datos. Este sistema carece de principios generales de protección en una norma superior a las sectoriales, así como de una autoridad superior que vele por la protección de los datos. De hecho, este sistema considera a las leyes ómnibus como obstaculizadoras de las relaciones

¹⁹ *Ibid.*, p. 112-113

²⁰ SALTOR, C.E., *op. cit.*, p. 114

²¹ PIÑAR MAÑAS, J.L., *op. cit.*, p. 86

comerciales internacionales, que impiden el libre flujo de información²².

En cuanto a Europa, se considera que la primera generación de leyes de protección de datos, fue fomentada por la Resolución 509 de la Asamblea del Consejo Europa sobre «los Derechos humanos y los nuevos logros científicos y técnicos»²³, y por el proyecto SAFARI, que surgió en la década de 1960 con el gobierno francés. Con él, se buscaba atribuir a cada ciudadano un número de identificación común para todas las relaciones con los departamentos administrativos del Estado. La publicación del informe denominado *La informatización de la sociedad* o informe *Nora y Minc*, permitió que los gobiernos europeos tomaran conciencia del peligro para la intimidad que implicaba la acumulación de datos personales mediante la tecnología y la informatización de la sociedad²⁴.

Así, surge en Europa una primera generación de leyes de protección de datos personales. Por ejemplo, Alemania, Francia, Dinamarca, Austria y Luxemburgo, dictan sus leyes de forma casi simultánea: la Ley del *Land de Hesse* de 1970, en Alemania, así como la propia Ley Federal alemana de 1977; en 1978 se aprueba la Ley francesa de Informática, Ficheros y Libertades; en 1978 se aprobaron en Dinamarca dos leyes, una sobre registros privados y otra sobre registros públicos; en 1978 se aprueba en Austria la Ley de Protección de Datos; y en 1979 se aprueba en Luxemburgo la Ley sobre utilización de datos en tratamientos informáticos. Asimismo, se produce alguna protección constitucional²⁵. En España, se empezó protegiendo la intimidad frente al uso de la informática mediante el art. 18.4 en 1978, y en Portugal, en 1976.

Un poco más tarde, el Tribunal Constitucional Alemán (en adelante, TCA) pronuncia su sentencia de 12 de diciembre de 1983. Esta sentencia declaró la Ley del Censo de Población parcialmente inconstitucional, porque obligaba a los ciudadanos a suministrar datos personales para fines estadísticos. Así, la sentencia reconoce el derecho fundamental a la “autodeterminación informativa” que supone la facultad de todo ciudadano de las sociedades democráticas de determinar qué, quién, cuándo y con qué

²² SALTOR, C.E., *op. cit.*, p. 109-111

²³ PIÑAR MAÑAS, J.L., *El Derecho a la autodeterminación informativa: Protección de datos: origen, situación actual y retos de futuro*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 85

²⁴ SALTOR, C.E., *op. cit.*, p. 66

²⁵ PIÑAR MAÑAS, J.L., *op. cit.*, p. 88

motivo puede conocer datos que le conciernen²⁶. En otras palabras, deriva de la idea de autodeterminación la facultad de decidir básicamente por sí mismo, cuándo y dentro de qué límites, procede a revelar situaciones referentes a la propia vida²⁷. Esta sentencia, junto a los principios aprobados por el Consejo de Europa, en el Convenio 108 de 1981, van a tener una influencia determinante en la promulgación de nuevas leyes. Surge así otra generación de leyes, que busca adaptar la legislación a los nuevos desafíos tecnológicos que plantea la década de 1980, y el matiz económico que presenta este fenómeno en la década de los 90. Así, cabe mencionar la *Data Protection Act* del Reino Unido de Gran Bretaña (1984); y en España, la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD), ya derogada y reemplazada por la Ley Orgánica de Protección de Datos de Carácter Personal 15/99 (LOPD) en diciembre de 1999²⁸. La protección de datos empieza así a concebirse como derecho fundamental, mediante construcción jurisprudencial. En España, cabe destacar las sentencias del Tribunal Constitucional número 290 y 292, ambas de 30 de noviembre de 2000²⁹.

En definitiva, en Europa, el desarrollo del derecho a la protección de los datos personales comienza en la legislación, sigue en las constituciones, y se desarrolla a través de la jurisprudencia y por la influencia de la acción del CdE; lo que unido a la necesidad de responder al desarrollo tecnológico, dará lugar a la evolución de las distintas generaciones de leyes, que finalmente en el ámbito de la Unión Europea serán uniformadas por la Directiva 95/46/CEE y sus modificatorias³⁰.

La técnica legislativa europea es de tipo ómnibus. Se basa en la búsqueda de una protección legislativa general de los datos de carácter personal, mediante la promulgación de una ley que contiene una serie de principios generales en la materia. En general, este sistema también crea una institución concebida como una “autoridad de aplicación con poder de policía tutelar”. Las siguientes características son propias de este sistema:

²⁶ Entre otros: PÉREZ LUÑO, E., “Estado constitucional y derechos de tercera generación”, *Anuario de filosofía del derecho* XVI, (1997), 545-570, p.555; ORTI VALLEJO, A., “El nuevo derecho fundamental (y de la personalidad) a la libertad informática”, *Derecho Privado y Constitución*, Núm. 2, enero-abril 1994, p.313

²⁷ SALTOR, C.E., *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina*, Tesis doctoral, Madrid, 2013, p. 57

²⁸ SALTOR, C.E., *op. cit.*, p. 68 y 69

²⁹ PIÑAR MAÑAS, J.L., *op. cit.*, p. 94 y 96

³⁰ SALTOR, C.E., *op. cit.*, p. 113

“1) existencia de reglas sustantivas generales aplicables al tratamiento automatizado de datos relativos a personas identificadas o identificables; 2) atribución de derechos a las personas titulares de los datos y de obligaciones a las personas responsables del fichero; 3) disposiciones especiales en el almacenamiento, colección, procesamiento y transmisión en los datos de carácter personal; 4) creación de una autoridad competente encargada de vigilar la aplicación de la ley”³¹.

2.3. NECESARIA APROXIMACIÓN INTERNACIONAL

La legislación tuitiva ofrecida por los Estados viene a ser insuficiente, ya que el avance tecnológico y las relaciones económicas confieren al problema una dimensión internacional. El flujo o circulación transfronteriza de datos personales ha supuesto una necesidad de regulación internacional, debido a las insuficiencias lógicas que presentaría abordarla de manera individual por cada uno de los Estados³². De ahí, nace el interés que ciertas Organizaciones Internacionales han prestado de cara a su regulación.

Estas Organizaciones, tanto universales como regionales, han adoptado diferentes instrumentos internacionales que han venido aproximándose a la materia desde sus orígenes, también desde el reconocimiento del derecho a la vida privada, y los factores que se relacionan con ella. Porque, como se ha explicado antes, es el derecho que se sitúa como antecedente a la protección de datos personales³³. No obstante, tras el paso del tiempo y el calado que el problema ha desarrollado en la actualidad, también han adoptado otros instrumentos que tratan más específicamente sobre la protección de datos personales y la tecnología, aunque en su mayoría no son jurídicamente vinculantes. Algunos ejemplos se exponen a continuación³⁴.

³¹ *Ibid.*, p. 110

³² GARZÓN CLARIANA, G. "La protección de los datos personales y la función normativa del Consejo de Europa", *Revista de Instituciones Europeas*, Vol 8. Nº.1, (enero-abril 1981), p.11

³³ En cuanto a las aproximaciones internacionales sobre el reconocimiento a la vida privada, pueden apreciarse diversos elementos que recogen expresamente este derecho o elementos relacionados con él. Así, el derecho a la vida privada goza de un reconocimiento expreso en el ámbito interamericano, mediante el artículo 11.2 de la Convención Americana sobre Derechos Humanos (Pacto de San José). En cuanto a Naciones Unidas y la regulación relacionada con la vida privada, destacan la Declaración Universal de Derechos Humanos de 1948 (art.12), la Convención sobre los Derechos del Niño de 1989 (artículo 16), la Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares de 1990 (artículo 14) y, la Convención de las Naciones Unidas contra la Corrupción de 2003 (art.10).

³⁴ Fuentes utilizadas, entre otras:

SALTOR, C.E., *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina*, Tesis doctoral, Madrid, 2013, p. 98-106

PIÑAR MAÑAS, J.L., *El Derecho a la autodeterminación informativa: Protección de datos: origen, situación actual y retos de futuro*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 85, 91-93

Documentos OEA, protección de datos. Disponible en

http://www.oas.org/es/sla/ddi/proteccion_datos_personales_documentos_OEA.asp, consultado el 16 de julio de 2017.

Naciones Unidas presenta un mayor recorrido sobre la preocupación específica por la incidencia del avance científico en los derechos humanos. Así, a título de ejemplo, destacan la Resolución de la Asamblea General, 2450 (XXIII), de 19 de diciembre de 1968, sobre Derechos Humanos y Progreso Científico, en la que establece la necesidad de fijar límites a las aplicaciones de la electrónica; la Resolución de la Asamblea General 45/95, de 14 de diciembre de 1990, sobre “los Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales”, o las Resoluciones de la Asamblea General 68/167, de 18 de diciembre de 2015, y 69/166, de 18 de diciembre de 2014 y 71/199, de 19 de diciembre de 2016, todas ellas sobre el “Derecho a la privacidad en la Era Digital”.

En el plano regional, y al margen de CdE (cuya acción en este ámbito será objeto de análisis en los próximos capítulos), la Organización de los Estados Americanos (OEA) también ha desarrollado elementos relacionados directamente con la protección de datos personales. Así, existen numerosas resoluciones de la Asamblea General, por ejemplo, la Resolución 2842 (XLIV-O/14) sobre Acceso a la información pública y protección de datos personales, la Resolución 2607 (XL-O/10) sobre la Ley Modelo Interamericana sobre Acceso a la Información Pública, o la Resolución 2514 (XXXIX-O/09) Acceso a la información pública: Fortalecimiento de la Democracia. También se han realizado numerosos estudios, por ejemplo, del Comité Jurídico Interamericano, (como CJI/RES. 212 (LXXXVI-O/15) Agenda Actual - Protección de Datos Personales, o CJI/RES. 186 (LXXX-O/12) Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas) o del Departamento de Derecho Internacional (como CP/CAJP-2921/10 rev.1 corr. 1 Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos (la Protección de Datos Personales)). Por otro lado, resaltan la African Union Convention on Cyber Security and Personal Data Protection, adoptada el 27 de junio de 2014, así como APEC - Border Privacy Rules System y APEC Privacy Framework, de 2005.

En cuanto a la Organización para la Cooperación y el Desarrollo Económicos (OCDE), destacan a modo de ejemplo las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, de 1980, adoptadas como una recomendación del Consejo de la OCDE, y actualizadas en 2013. También, el 11 de abril de 1985 los

ministros de la OCDE adoptaron la Declaración sobre flujos de datos transfronterizos. En la conferencia ministerial de la OCDE “Un mundo sin fronteras: determinación del potencial del comercio electrónico”, celebrada en 1998 en Ottawa, se llevó a cabo la Declaración ministerial sobre la protección de la privacidad de las redes globales. Asimismo, resaltan las Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad, que se adoptaron como Recomendación del Consejo de la OCDE en su sesión 1037 de 25 de julio de 2002.

En el Derecho de la Unión Europea, destacan los siguientes instrumentos. En primer lugar, la Directiva 95/ 46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hace énfasis en el marcado carácter económico de los datos, garantizando la libre circulación de los mismos. A partir del 2000, se dio un paso importante con la elevación del derecho a la protección de datos personales como derecho autónomo en el artículo 16 del TFUE, y como derecho fundamental en el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, también diferenciado del derecho a la vida privada y familiar (art. 8). Posteriormente, la Unión Europea llevó a cabo una importante actividad legislativa en la materia. Así, cabe destacar la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, y el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

2.4. DEFINICIÓN DEL CONCEPTO

Toda esta problemática vinculada a la protección de datos personales no es para nada sencilla, y la doctrina se ha hecho eco de esta dificultad. Tanto en América como en Europa, los autores han reflexionado a cerca de su naturaleza y a cerca del *nomen iuris* que ilustre lo mejor posible su contenido. A grandes rasgos, las posiciones conceptuales y terminológicas de la protección de datos pueden definirse en dos corrientes: aquellas elaboraciones teóricas que pretenden extender el derecho a la intimidad a toda

información personal, y aquellas que abogan por la identificación de un bien jurídico autónomo (y, por tanto, un derecho autónomo) denominado de diferentes maneras “— intimidad informativa, libertad informática o autodeterminación informativa—”³⁵.

La posición doctrinal de Estados Unidos responde claramente a la primera corriente. Por regla general defiende el derecho fundamental de la *privacy*, o sea, sin autonomía propia. Sin embargo, ello no le quita fundamento constitucional a la tutela frente a la informática, “pues el atentado sigue siendo a un derecho fundamental, cual es la *privacy*”³⁶. COLIN BENNET define *privacy* como “el resultado de la acción de los poderes públicos y de los propios ciudadanos a través de sus organizaciones y asociaciones y de otras entidades comprometidas con la defensa de los derechos humanos o con los de los consumidores y usuarios”³⁷.

La posición de la doctrina en Europa suele situarse en torno a la segunda línea comentada. Los autores alemanes normalmente defienden la autonomía del derecho, debido al precedente de la citada sentencia del TCA. Así, destaca PODLECH, y DENNINGER “en cuanto al contenido del derecho a la autodeterminación informativa, aclara que la revelación y el uso de los datos personales, abarca todas las fases de elaboración y uso de datos, o sea, acumulación, transmisión, modificación y cancelación”³⁸.

En la doctrina italiana cabe destacar a FROSINI, que defiende la llamada libertad informática. La califica de “derecho perteneciente a la personalidad moral, definiéndolo como el derecho de disponer de los propios datos personales, esto es, de controlar la veracidad o exactitud, de impedir la difusión si se trata de datos sensibles o reservados, de verificar la utilización para el fin autorizado”³⁹.

Finalmente, los autores españoles, aunque divididos, normalmente defienden la autonomía del derecho a la autodeterminación informativa o protección de datos personales, con clara influencia alemana. Entre ellos destacan PÉREZ LUÑO,

³⁵MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p.17

³⁶ORTI VALLEJO, A, *op.cit.*, p. 313, 314

³⁷MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 74

³⁸ORTI VALLEJO, A, *op.cit.*, p. 313

³⁹ORTI VALLEJO, A, *op.cit.*, p. 316

MURILLO DE LA CUEVA, PIÑAR MAÑAS, DAVARA RODRIGUEZ⁴⁰, o SALTOR⁴¹; y otros con posiciones algo divergentes como ORTI VALLEJO o REBOLLO DELGADO⁴², como veremos a continuación.

En concreto, para MURILLO DE LA CUEVA, hay igualdad entre los términos de protección de datos personales o derecho a la autodeterminación informativa⁴³. Dependiendo de la obra, utiliza un término u otro⁴⁴. Asimismo, defiende la insuficiencia del derecho a la intimidad para recoger este nuevo derecho: “los rasgos indicados del derecho a la intimidad no permiten responder a los riesgos que proceden de la recopilación, tratamiento, almacenamiento y transmisión de datos personales por medio de las posibilidades que ofrecen la informática y la telemática o, si se prefiere, las Tecnologías de la Información y de las Comunicaciones”⁴⁵. Finalmente, para este autor, lo importante es identificar la protección de datos o autodeterminación informativa como un derecho fundamental y recoger su contenido:

“Entre los elementos que lo componen nos encontramos, ante todo, con la exigencia del consentimiento informado del afectado como regla que ha de observarse antes de proceder a un tratamiento de este tipo de datos. Consentimiento que solamente puede ser obviado cuando la ley así lo permita. Luego, está el reconocimiento a todos de facultades positivas y negativas sobre la información personal que les afecta y que sea objeto de tratamiento o se halle en ficheros automatizados. Es decir, el derecho a conocer la existencia de ficheros en los que se tratan datos personales y, en particular, los derechos a acceder a los que se refieran al afectado, rectificar los incorrectos y cancelar los excesivos, inadecuados a la finalidad para la que se recabaron u obtenidos en violación de las normas legales. Como es natural, a estos derechos de los titulares de

⁴⁰ *Ibid.*, p. 317, 318

⁴¹ SALTOR, C.E., *op. cit.*, p. 74 y 60

⁴² Otra forma de concebirlo es que la autodeterminación informativa integra el aspecto o concepto subjetivo del derecho a la intimidad. En primer lugar, se distingue el ámbito objetivo y el subjetivo de la intimidad: el concepto objetivo atiende en esencia a la etimología del concepto como una “zona espiritual reservada o íntima de una persona o de un grupo, especialmente de una familia”, y el concepto subjetivo supone “la facultad del individuo derivada de la idea de autodeterminación, de decidir básicamente por sí mismo, cuándo y dentro de qué límites procede a revelar situaciones referentes a la propia vida”. SALTOR, C.E., *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina*, Tesis doctoral, Madrid, 2013, p. 57

⁴³ MURILLO DE LA CUEVA, P.L., “El derecho a la autodeterminación informativa y la protección de datos personales”, *Azpilcueta*, N.º. 20, 2008, p.2

⁴⁴ “He utilizado para denominarlo la expresión Derecho de la Protección de Datos Personales, pues me parece que cuenta ya con la densidad necesaria para ser contemplado como un sector material específico y esa fórmula ayuda a identificarlo ya que responde a sus contenidos, particularmente al bien jurídico que pretende preservar y a la técnica que para ello emplea”. MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 7; “Personalmente, he preferido hablar de autodeterminación informativa por- que, si bien se trata de una fórmula poco estética, es, sin embargo, más precisa pues apunta al núcleo del derecho, a su aspecto sustantivo, mientras que la protección de los datos personales es su manifestación instrumental y, por eso, tiene un carácter técnico que le priva de capacidad significativa” MURILLO DE LA CUEVA, P.L., “El derecho a la autodeterminación informativa y la protección de datos personales”, *Azpilcueta*, N.º. 20, 2008, p.44.

⁴⁵ MURILLO DE LA CUEVA, P.L., “El derecho a la autodeterminación informativa y la protección de datos personales”, *Azpilcueta*, N.º. 20, 2008, p. 47

los datos personales, corresponden los correlativos deberes de quienes los acopian, tratan, transmiten, conservan o utilizan de cualquier manera”⁴⁶.

PIÑAR MAÑAS explica que la autodeterminación informativa y la protección de datos son derechos fundamentales autónomos e independientes al derecho a la intimidad. Si bien, la autodeterminación informativa es sucedida por la protección de datos, como consecuencia del uso de los dispositivos informáticos y del valor económico que tiene desde los años 90. Así, defiende que el derecho se fundamenta “en el poder de disposición de los datos personales por su titular, y en que tales datos son sometidos a tratamiento. Lo que se traduce en que por definición quien trata datos personales trata datos ajenos, no propios, que debe utilizar con estricto respeto a los derechos del interesado. Esta construcción nos reconduce al respeto a la dignidad de la persona, base fundamental de la protección de datos”⁴⁷.

Por su parte, PÉREZ LUÑO establece la siguiente secuencia: en el Estado liberal de Derecho aparecen los derechos de primera generación (libertades fundamentales de signo individual, cuyo valor guía fue la libertad), en el Estado social y democrático de Derecho aparecen los derechos de segunda generación (económicos, sociales y culturales, cuyo valor guía fue la igualdad), y en el Estado constitucional de Derecho aparecen los derechos de tercera generación (entre ellos el derecho a la paz, calidad de vida, de los consumidores, o a la libertad informática; cuyo valor guía es la solidaridad y cooperación). Según él, aparecen como una respuesta a la “contaminación de las libertades”⁴⁸. Su definición puede resumirse en “la libertad informática, que aparece como un nuevo derecho de autotutela de la propia identidad informática, o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico”⁴⁹, cuyos principales instrumentos de tutela suelen ser “un status de habeas data, concretado en las garantías de acceso y control a las informaciones procesadas en bancos de datos por parte de las personas concernidas”, y un “status activus processualis, como el reconocimiento de la facultad de cada persona para participar activamente y asumir su propia responsabilidad en los procedimientos que le afectan, así

⁴⁶ MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. y 5

⁴⁷ PIÑAR MAÑAS, J.L., *El Derecho a la autodeterminación informativa: Protección de datos: origen, situación actual y retos de futuro*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p.88-103

⁴⁸ PÉREZ LUÑO, A.E., “Estado constitucional y derechos de la tercera generación”. Universidad de Sevilla. *Anuario de filosofía del Derecho* XIV (1997), 545-570, p. 564

⁴⁹ PÉREZ LUÑO, A.E., “La tutela de la libertad informática en la sociedad glocalizada”, *ISEGORIA* 22 (2000) pp.59-68, p. 59

como en el seno de las estructuras organizativas más directamente vinculadas con el ejercicio de los derechos fundamentales”⁵⁰.

Finalmente, para ORTI VALLEJO, “[e]l conflicto de intereses expuesto, pone en evidencia que no estamos ante un nuevo problema, sino ante el ya conocido enfrentamiento entre la intimidad, honor, etc., y el derecho a la información. Sólo se trata de una nueva tecnología, una nueva posibilidad de atentar contra diversos derechos de la persona, especialmente la intimidad, que a lo sumo plantea un enfoque renovado del concepto de la intimidad”. Para este autor, la solución pasa por “reconocer, la necesidad de la recogida de las informaciones personales, y de otra, por conceder eficaces instrumentos de control; no se puede configurar el derecho a la intimidad como derecho a ser dejado en paz, sino como el poder de controlar el uso que otros hagan de las informaciones relativas a un determinado sujeto”⁵¹.

⁵⁰ PÉREZ LUÑO, A.E., “Las Generaciones de Derechos Humanos”, *Revista del Centro de Estudios Constitucionales* 203, Núm. 10. Septiembre-Diciembre 1991, p.208, 212, 213.

⁵¹ ORTI VALLEJO, A, *op. cit.*, p. 325, 326

III. LA PROTECCIÓN DE DATOS PERSONALES EN EL SENO DEL CONSEJO DE EUROPA

Después de contextualizar la problemática de la protección de datos en general y antes de analizar la Jurisprudencia del TEDH en materia de protección de datos personales, conviene en primer lugar realizar un breve recorrido cronológico sobre la actividad del Consejo de Europa en este ámbito. Se señalarán en cada caso, los hitos paralelos más importantes de la jurisprudencia del TEDH sobre la materia, para tener una visión más integrada.

3.1. UN RECORRIDO HISTÓRICO

El punto inicial de este recorrido histórico, viene marcado por el Convenio Europeo de Derechos Humanos (en adelante, CEDH). Este Convenio dispuso en su artículo 8.1 que “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”. Pero debido al paso del tiempo y la evolución tecnológica de la sociedad, en 1967 se puso de manifiesto en la Asamblea Consultiva del CdE (porque posteriormente adoptaría el nombre de Asamblea Parlamentaria) la preocupación por la incidencia de ciertos logros de la ciencia, la técnica y la informática en el respeto de los derechos humanos. Se consideró que la protección ofrecida por el art. 8 podría resultar insuficiente, ya que, a fecha de la redacción del Convenio, no se pudo prever el crecimiento exponencial de la tecnología, y las implicaciones que ésta tendría respecto de la posible vulneración del derecho. De esta manera, ya en 1968, la Asamblea Parlamentaria hizo un llamamiento al Comité de Ministros para que examinara si las legislaciones internas de los Estados miembros protegían adecuadamente el derecho de los individuos al respeto de su vida privada ante el desarrollo que se había dado en cuanto las tecnologías informáticas⁵². El estudio⁵³ demostró que las legislaciones nacionales no estaban plenamente adaptadas a los cambios introducidos por las nuevas tecnologías de la información, por lo que se constituyó un Comité Intergubernamental de Expertos

⁵² CONSEJO DE EUROPA, Asamblea Parlamentaria, Recommendation 509 (1968) on human rights and modern scientific and technological developments, de 31 de enero de 1968

⁵³ Assemblée Consultative, Commission juridique, Rapport sur les droits de l'homme et les réalisations scientifiques et technologiques modernes (rapporteur: M.CZERNETZ). Documents de séance, Doc.2326, 22 Janvier 1968;

encargado de elaborar medidas apropiadas a nivel regional europeo⁵⁴. Es decir, desde 1969, se empezó a evidenciar que el art. 8 CEDH no protegía de forma suficiente a los individuos frente al uso abusivo de la informática.

En 1973 y 1974 se adoptó un primer paso en la dirección de colmar sus lagunas, con la adopción de las Resoluciones (73) 22 y (74) 29 del Comité de Ministros, que establecieron principios para la protección de datos personales en bancos de datos automatizados del sector privado y del sector público. El objetivo era poner en marcha el desarrollo de una legislación nacional basada en estas resoluciones⁵⁵. Estas resoluciones enunciaban una serie de principios básicos, dejando una absoluta libertad a los Estados miembros para que las adoptasen en el derecho interno por vía legislativa o reglamentaria. A pesar de su relativa modestia, estas Resoluciones adquieren una significación histórica: son los primeros textos internacionales que presentan a los Estados pautas de conducta sobre la materia de protección de datos⁵⁶. Sin embargo, durante la preparación de estos textos se puso de manifiesto que la protección integral de los datos personales sólo sería eficaz si se reforzaban dichas normas nacionales mediante normas internacionales vinculantes. La misma sugerencia se había hecho en la Conferencia de Ministros Europeos de Justicia en 1972⁵⁷.

En febrero de 1976, el Comité de Ministros del C.d.E. adoptó la Resolución (76) 3, constituyendo un Comité de Expertos de protección de datos encargados de estudiar la conveniencia de elaborar o bien una convención que desarrollara el artículo 8 del Convenio Europeo de Derechos Humanos garantizando la protección de datos personales, o bien un protocolo que ampliara tal artículo. Se optó por la convención, y se procedió a elaborar el Convenio sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, conocido finalmente como Convenio 108⁵⁸.

Dos años después de esa resolución, se produjo el primer antecedente jurisprudencial en el TEDH (aunque aún muy indirecto) sobre la materia en cuestión. El 6 de septiembre de

⁵⁴KINOSHITA F., MÉNDEZ PINEDO, A., “Transmisión internacional de datos personales”, 2000. Disponible revista electrónica http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5568. Consultado el 5 de Mayo de 2017.

⁵⁵COUNCIL OF EUROPE, “Background, Convention 108 and Protocol”. Disponible en <<http://www.coe.int/en/web/data-protection/background>> Consultado el 5 de Mayo de 2017.

⁵⁶KINOSHITA F., MÉNDEZ PINEDO, A., *op.cit.*

⁵⁷COUNCIL OF EUROPE, “Background, Convention 108 and Protocol”, *op. cit.*

⁵⁸KINOSHITA F., MÉNDEZ PINEDO, A., *op.cit.*

1978, dictó la sentencia en el caso *Klass and others c. Alemania*, en el contexto de la posible vulneración del derecho al respeto a la vida privada y familiar, domicilio y correspondencia (art. 8 CEDH), a través de la interceptación de las comunicaciones, *tapping* telefónico y vigilancia secreta⁵⁹. Como se verá más adelante, será la elaboración jurisprudencial en la tutela de este derecho la vía por la que el Tribunal llegará al reconocimiento de la protección de los datos personales.

Entre tanto, se seguía con la redacción del Convenio 108, que se prolongó hasta 1980. El Convenio se abrió a la firma el 28 de enero de 1981 y fue el primer instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos. El Convenio entró en vigor el 10 de octubre de 1985, al cumplirse el requisito de su firma y ratificación por cinco Estados Parte. En virtud de este Convenio, las Partes Contratantes se obligan a adoptar las medidas necesarias en su legislación interna para aplicar los principios que en él se establecen para garantizar el respeto en su territorio de los derechos humanos fundamentales de todas las personas en lo que respecta al tratamiento de los datos personales. Estos principios se refieren, en particular, a la recolección justa y lícita y al tratamiento automático de los datos, al almacenamiento con fines legítimos y específicos y no a fines incompatibles con estos fines, ni conservados durante más tiempo de lo necesario. Se refieren también a la calidad de los datos, en particular que deben ser adecuados, pertinentes y no excesivos (proporcionalidad), la exactitud de los mismos, la confidencialidad de los datos sensibles, la información del interesado, y su derecho de acceso y rectificación, y la libre circulación de datos personales entre los Estados Partes en la Convención, entre otros⁶⁰.

Unos años más tarde, se produjo el primer antecedente jurisprudencial directo sobre la protección de datos personales. Hablamos del asunto *Leander v. Sweden* de 1987, referido al almacenamiento de datos en registros secretos. Sin embargo, la sentencia no viene acompañada de una elaboración jurisprudencial relevante. No formula en su sentencia en qué consisten los datos de carácter personal, ni su protección, ni la existencia de una nueva área autónoma dentro del art. 8 CEDH. Simplemente, el Tribunal se limita a otorgar protección a los datos de carácter personal que aparecen en el supuesto de hecho, pero lo

⁵⁹ TEDH: *Data protection*, Factsheet, p.2. Disponible en http://www.echr.coe.int/Documents/FS_Data_ENG.pdf. Consultado el 17 de julio de 2017.

⁶⁰ COUNCIL OF EUROPE, “Background, Convention 108 and Protocol”, *op.cit.*

tutela refiriéndose a la protección del derecho al respeto de la vida privada de manera genérica. Lo mismo sucede en el caso *Gaskin c. Royaume Uni*, de 1989, donde, además, evita pronunciarse sobre un derecho de acceso a los datos personales en expedientes administrativos, posiblemente amparado por la protección de la vida privada del art. 8. Es decir, es obvio que ese derecho de acceso se derivaría de manera directa de esa nueva área de protección de los datos personales, pero no se pronuncia sobre ello. Quizá, también, precisamente para evitar pronunciarse sobre la autonomía de la protección de datos personales dentro del derecho al respeto a la vida privada. De hecho, tampoco toma en consideración el Convenio núm. 108, ya en vigor. Como se ha explicado, este instrumento explica en detalle qué son los datos de carácter personal y cómo se deben proteger. Sin embargo, el Tribunal, a pesar de haber examinado supuestos en los que se planteaba el uso de datos personales o se discutía sobre el acceso a datos contenidos en expedientes personales (elementos contemplados en el Convenio 108), decide obviar su mención hasta finales de siglo.

Desde la conclusión del Convenio 108, como ya se ha visto, la sociedad empezó a transformarse completamente. El desarrollo social y económico empezó a llevar a formas aún más complejas de organización, gestión y producción, basadas en poderosos sistemas de procesamiento. En este contexto, el individuo se convierte en un agente activo de la “sociedad de información”, al mismo tiempo que su privacidad es objeto de una injerencia aún mayor por parte de los sistemas de información de numerosos servicios públicos y privados –bancos, servicios de créditos, asistencia social, seguros, policía, atención médica...-. Esta evolución constituye un enorme desafío en materia de protección de datos, y la experiencia demostró que ni los principios del Convenio ni los reglamentos nacionales sobre protección de datos podían regular exactamente cada situación en la que se recopilaban datos personales en los diferentes sectores mencionados. Por lo tanto, para cada uno de los diferentes sectores hubo que profundizar en los principios de este tratado. En lugar de enmendar el Convenio o añadir protocolos al mismo, el Consejo de Europa optó por utilizar otro instrumento para este fin: el de las recomendaciones a los gobiernos. Éstas, en vez de la firma y ratificación por cada uno de los Estados miembros, sólo requieren la aprobación unánime del Comité de Ministros y por lo tanto es más fácil adaptarlos a circunstancias cambiantes antes que modificar convenios⁶¹. Aunque, por otra

⁶¹ COUNCIL OF EUROPE, “Background, Convention 108 and Protocol”, *op.cit.*

parte, podría apreciarse que, frente a esta ventaja, está el perjuicio de la falta del carácter obligatorio de las recomendaciones frente a los convenios. Estas recomendaciones, como bien ha descrito Pavón Pérez, “son de carácter sectorial y versan sobre temas específicos que cubren cada uno de los aspectos necesitados de protección, luego versan sobre cuestiones amplias y diversas”⁶². Asimismo, además de las recomendaciones, la actividad del Consejo de Europa en materia de protección de datos personales se vio convenientemente desarrollada por una serie de Informes⁶³ encargados a los expertos de la Organización que incidían en los extremos más necesitados de protección⁶⁴.

En este orden de cosas, es necesario destacar que a finales del s. XX (año 1997), en el caso *Z c. Finlandia*, el Tribunal se aproximó a las cuestiones planteadas en casos anteriores, pero, esta vez sí, desde la perspectiva de la protección de datos personales como elemento integrado en el art. 8 CEDH. Es, por tanto, el momento del reconocimiento de la materia por el Tribunal. Es decir, en los casos expuestos anteriormente, el Tribunal evitaba pronunciarse sobre la existencia de la protección de datos personales como área autónoma de protección, dentro del derecho al respeto de la vida privada. Pero en este caso, por primera vez, el TEDH se refiere a la protección de datos personales expresamente como área integrada en el art. 8 CEDH. Así, el Tribunal, fundándose en la Recomendación del Comité de Ministros del Consejo de Europa, (89) 14 sobre las incidencias éticas de la infección por VIH en el marco sanitario y social⁶⁵, concibe esos datos de carácter médico como datos de carácter personal, necesitados de protección dentro del art. 8 CEDH. Este planteamiento contrasta con los casos anteriores, en los que el Tribunal obviaba mencionar la autonomía de los datos personales, imbricando el supuesto de hecho en el derecho al respeto a la vida privada de manera

⁶² Por ejemplo, Recomendación Núm. R (90) 19, relativa a la protección de datos personales utilizados en investigaciones científicas y estadísticas. Adoptada por el Comité de Ministros el 23 de septiembre de 1983; Recomendación Núm. R (97) 18 sobre la protección de datos personales recopilados y tratados con fines estadísticos. Adoptada por el Comité de Ministros el 30 de septiembre de 1997; Recomendación Núm. R (81) 1, relativa a la reglamentación aplicable a los bancos de datos médicos automatizados. Adoptada por el Comité de Ministros el 23 de enero de 1981; Recomendación Núm. R (87) 15, regulando el uso de datos personales en el sector de la policía. Adoptada por el Comité de Ministros el 17 de septiembre de 1987; Recomendación Núm R (83), relativa a la protección de los usuarios de servicios de informática jurídica. Adoptada por el Comité de Ministros el 22 de febrero de 1983. Más recientemente, la evidente e innegable relación existente entre la protección de datos personales e Internet ha quedado explicitada en la Recomendación Núm. R (99) 5 relativa a la protección de la vida privada en Internet adoptada por el Comité de Ministros el 23 de febrero de 1999.

⁶³ Rapport sur “la protection des donnés à caractere personnel concernant l’utilisations de cartes à puces”, (2201); Rapport sur “les contrats encadrant les transferts des donnés à caractère personnel entre les Parties à la Convention STE n.º 108 et les pays tiers n’offrant pas un niveau de protection adéquat” (2001) preparado G. Buttarelli; Rapport sur “les données sensibles revisitées” (1999), preparado por Spiros Simitis y J. W. Goethe.

⁶⁴ PAVÓN PÉREZ, J.A., “La Protección de Datos Personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales”, *Anuario de la Facultad de Derecho*, ISSN 0213-988X, N.º 19-20, 2001-2002, p. 240

⁶⁵ CONSEJO DE EUROPA, Comité de Ministros, Recommendation R (89)14 sur les incidences éthiques de l’infection VIH dans le cadre sanitaire et social, Doc. CM/Rec(89)14, de 24 de octubre de 1989

genérica y global. Por otra parte, cabe destacar que no sólo se produjo este avance, sino que este reconocimiento de la protección de datos personales vendrá acompañado de la mención al Convenio 108. Esta mención supone que debe equipararse la tutela de la vida privada que el derecho nacional debe desplegar, con la otorgada por las previsiones del Convenio 108⁶⁶. En otras palabras, dado que este tratado explica en detalle las medidas de protección que los Estados deben proporcionar para una adecuada tutela de los datos de carácter personal, el Tribunal se hace eco de las disposiciones del Convenio 108 relativas a este aspecto, para trasladar al Estado demandado cómo debe ser la protección que debe otorgar a los datos personales para hacer efectivo el derecho consagrado en el art. 8 CEDH. Ya que, ahora sí, los datos personales se configuran como un elemento integrado dentro del derecho al respeto de la vida privada y familiar.

El 8 de noviembre de 2001 se adoptó el Protocolo Adicional al Convenio 108, relativo a las autoridades de control y a los flujos transfronterizos de datos personales, que fue abierto a la firma en noviembre del mismo año y entró en vigor en julio de 2004. Este protocolo versa sobre la obligación de los Estados partes de establecer una garantía institucional u organismo independiente de control para supervisar la aplicación de los derechos reconocidos en el Convenio 108. Y, por otra parte, pretende establecer una serie de cautelas en relación con el flujo transfronterizo de datos personales a Estados u organizaciones privadas que no proporcionan un nivel adecuado de protección⁶⁷.

Finalmente, debido a la creciente revolución tecnológica y al mundo globalizado del s. XXI, ya desde 2010, se consideró necesario modernizar el Convenio 108, por una parte, para abordar mejor los desafíos derivados de la utilización de las nuevas tecnologías de la información y la comunicación y, por otra, para reforzar la aplicación del Convenio 108. La labor de modernización se inició con la preparación de un informe encaminado a identificar las áreas en las que sería necesario modernizar la Convención 108 para hacer frente a los nuevos desafíos, y con la consulta lanzada por el Secretario General del C.d.E. con múltiples interesados con ocasión de la 5ª edición del día de protección de datos y el 30º aniversario de la Convención 108 el 28 de enero de 2001. En estos momentos, la Comisión *ad hoc* sobre protección de datos (*Ad hoc* Committee on Data Protection,

⁶⁶ MARTÍNEZ MARTINEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Colección “Protección de datos”, THOMSON CIVITAS, 2004, p. 199.

⁶⁷ RUÍZ MIGUEL, C., *op.cit.*, p.12

CAHTA), es responsable de la modernización de la Convención 108 y su Protocolo⁶⁸, cuyo borrador está ya publicado⁶⁹.

Una vez planteado este recorrido histórico por la acción del C.d.E. en materia de protección de datos, parece necesario detenerse en sus hitos más importantes, como son el Convenio 108 y su Protocolo Adicional, resultando también de interés mencionar aquellas áreas necesarias de modernización para la adecuada protección de datos personales ante los nuevos retos a la privacidad que plantea la actualidad. Porque, como se verá en el siguiente capítulo, tendrá una influencia directa sobre la jurisprudencia del TEDH en la materia objeto de estudio.

3.2. EL CONVENIO 108 PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL (1981)

Conviene recordar el contexto en el que se gesta este Convenio, para entender su alcance y limitaciones. Como se ha explicado anteriormente, el crecimiento del uso de la informática y tecnología con respecto al tratamiento automatizado de datos personales había generado un “poder de información” innegable, que suponía una responsabilidad social de los detentadores de esa información tanto en el sector público como en el privado. Esa responsabilidad social abarcaba ciertas obligaciones lógicas subsecuentes como la obtención de una información de calidad, abstenerse de almacenar información innecesaria al propósito concreto, así como de la relevación de la información no autorizada, o la protección física de la misma, entre otras.

Los Estados, por regla general, hemos visto que tenían sistemas legales que no estaban enteramente desprovistos de normas que ayudasen a cumplir estos objetivos, pero surgieron otra serie de materias o problemas prácticos que las legislaciones internas no habían resuelto, de ahí la necesidad de adoptar un Convenio internacional. Así, por ejemplo, la falta de reglas generales de almacenamiento, o el control del individuo de su

⁶⁸ COUNCIL OF EUROPE, “Background, Convention 108 and Protocol”, *op. cit.*

⁶⁹ Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. Disponible en <https://rm.coe.int/16806a616c>. Consultado el 17 de julio de 2017.

propia información usada por terceros, son algunas de las causas que llevaron a la necesidad de crear el Convenio.

Asimismo, el procesamiento de datos automático afectaba a partes ubicadas en diferentes países, lo que suponía una dificultad para determinar el Estado que tenía jurisdicción ante un posible conflicto y qué ley estatal era aplicable. Además, debido al desarrollo del tráfico internacional de datos, era necesario crear mecanismos a nivel internacional que permitieran a los Estados mantenerse recíprocamente informados y poder hacerse consultas entre ellos sobre materias de protección de datos⁷⁰.

Por tanto, este acuerdo internacional pretendía, sobre todo, reforzar esa legislación nacional de protección de datos que nació progresivamente tras las Resoluciones (73) 22 y (74) 29 del Comité de Ministros, en aquellos aspectos que no regulaban y en los que era necesaria una cooperación internacional⁷¹. La manera en que se llevó a cabo, se expondrá a continuación, deteniéndonos primero en algunos aspectos formales de este tratado.

3.2.1. Forma

A pesar de que el Consejo de Europa es una Organización Internacional de ámbito regional, este instrumento fue denominado “Convención” (en lugar de Convención Europea), con el ánimo de permitir la adhesión de Estados no europeos (arts. 24 y 25)⁷². Por tanto, puede concluirse que el objetivo del CdE en la elaboración de este instrumento fue concebirlo con alcance mundial.

El procedimiento de adhesión de los Estados no europeos puede llevarse a cabo de dos maneras: bien el Comité de Ministros invita a un Estado no miembro a acceder a la Convención, bien el acceso es solicitado directamente por los Estados no miembros interesados sin necesidad de invitación. En todo caso, antes de poner sobre la Agenda del Consejo de Ministros el acceso de cierto Estado, se conocerá informalmente la opinión de los Estados miembros y no miembros, que sean parte de la Convención. Finalmente,

⁷⁰ Memoria explicativa del Convenio 108 sobre el Tratamiento automatizado de datos de carácter personal, del Consejo de Europa, págs. 1-3. Disponible en <https://rm.coe.int/16800ca434>. Consultado el 26 de junio de 2017.

⁷¹ *Ibid.*

⁷² *Ibid.*, págs. 6, pár. 24.

la decisión debe ser acordada por unanimidad por los miembros del Consejo de Europa que hayan ratificado la Convención⁷³.

Actualmente hay 50 Estados Parte en el Convenio. Todos los Estados miembros del Consejo de Europa son parte de la Convención, y cabe resaltar que sólo hay tres Estados no miembros del Consejo de Europa que son parte en la misma: Mauritania, Senegal, y Uruguay⁷⁴. Un hecho importante es, que, en junio de 1999, el Comité de Ministros del Consejo de Europa aprobó enmiendas al Convenio 108 que permiten a la Unión Europea adherirse a este tratado. Para entrar en vigor, estas enmiendas deben ser aceptadas por todos los Estados Partes en el Convenio y, actualmente, hay 44 partes que han aceptado las enmiendas que permiten a la U.E. adherirse⁷⁵.

La expansión de la Convención 108 fuera de Europa es ahora más importante, y tiene más sentido, debido al aumento de los países con leyes de privacidad de datos, y particularmente de países fuera de Europa, en las últimas décadas (como se ha visto en apartados anteriores⁷⁶). A pesar de este crecimiento de leyes fuera de Europa en la materia, sería poco realista sugerir que otras tantas nuevas adhesiones al Convenio 108 sean posibles o deseables, según los objetivos del mismo. Muchas de estas leyes no comprenden los requisitos del Convenio 108, incluso por razones tan importantes como de déficits democráticos, cuestiones constitucionales, falta de una autoridad de protección de datos y otras cuestiones que no tienen fácil solución. A pesar de esta consideración, el ánimo de alcance global es claro⁷⁷. En este sentido, lo que se viene haciendo de cara a potenciar este Convenio como un estándar internacional y su ratificación por los distintos países, es invitarles a considerar seriamente las ventajas e implicaciones potenciales de hacerlo, ya que éstas variarán de un país a otro y cada uno de ellos requerirá una evaluación equilibrada de los intereses de ese país y su gobierno, de sus empresas, y

⁷³ Secretariat of the Convention's Consultative Committee Directorate General of Human Rights and Rule of Law, "Accession to Convention 108 and to its additional Protocol by non-European States", 2011. Disponible en <http://www.coe.int/en/web/data-protection/articles-speeches-and-presentations>. Consultado el 1 de julio de 2017.

⁷⁴ Treaty Office del Consejo de Europa, "Chart of signatures and ratifications of Treaty 108" (Status as of 01/07/2017). Disponible en http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=MOQhGjyo. Consultado el 1 de Julio de 2017.

⁷⁵ *Ibid.*

⁷⁶ Para ver una relación de los países con leyes de privacidad de datos y una comprensión mayor de la globalización de esta materia, visitar: GRAHAM GREENLEAF, "Balancing globalisation's benefits and commitments: accession to data protection convention 108 by countries outside europe", The global context of Convention 108 'globalisation', Conference Presentation, 2016, págs. 2-3. Disponible en <http://www.coe.int/en/web/data-protection/articles-speeches-and-presentations>. Consultado el 1 de julio de 2017.

⁷⁷ *Ibid.*, p. 3

ciudadanos⁷⁸. Así, es necesario que antes de ser Parte estén bien informados sobre la misma y consideren cuidadosamente los beneficios potenciales de la adhesión⁷⁹.

Por otra parte, el Convenio 108 del Consejo de Europa fue el primer instrumento internacional jurídicamente vinculante, que aborda explícitamente la protección de datos⁸⁰, aunque se limita a formular una serie de principios fundamentales, a modo de mínimos, que se resumen en la especificación o limitación del propósito de toma de datos, calidad y seguridad de los datos, acceso y rectificación individual, supervisión independiente, transparencia y reparación.⁸¹ Así, cada Parte debe adoptar las medidas necesarias para dar efecto a los principios mínimos que contiene el Convenio, en su legislación interna, con libertad de forma de aplicación.

3.2.2. Contenido

En primer lugar, la idea vertebral del Convenio es establecer un equilibrio entre dos factores. Por un lado, la protección de la vida privada, con relación al tratamiento automático de los datos de carácter personal. Y por otro, la liberalización de los flujos de datos entre los Estados parte o “*ius communicationis*”⁸², en palabras de Garzón Clariana, la liberalización *de iure* de las corrientes de datos personales entre los Estados partes “en favor de la libertad de información sin consideración de fronteras”⁸³. Así, cuando la Convención impone ciertas restricciones o condiciones al ejercicio de la libertad de información (art. 10 CEDH), sólo lo hace en la medida estrictamente justificada para la protección de otros derechos y libertades individuales⁸⁴. Esta idea se concibe *a priori* para las personas físicas, pero también permite el Convenio la extensión a las personas jurídicas. Y se aplica tanto al sector público como al privado, abarcando todos los sectores de la sociedad.

⁷⁸ *Ibid.*, p. 4.

⁷⁹ *Ibid.*, p. 9.

⁸⁰ AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, CONSEJO DE EUROPA, “Manual de legislación europea en materia de la protección de datos”, Belgium, 2014. p. 14. Disponible en <http://www.coe.int/en/web/data-protection/home>. Consultado el 1 de julio de 2017.

⁸¹ Jörg Polakiewicz, “International Data Protection Conference Convention 108 as a global privacy standard?”, 17 June 2011. Disponible en <http://www.coe.int/en/web/data-protection/articles-speeches-and-presentations>. Consultado el 26 de junio de 2017.

⁸² ORTEGA JIMÉNEZ, A., *op.cit.*, p. 49.

⁸³ GARZÓN CLARIANA, G., *op.cit.*, p. 16.

⁸⁴ Memoria explicativa del Convenio 108., *op.cit.*, pág. 1-3.

La definición de datos personales que el Convenio ofrece, requiere de varias apreciaciones. En primer lugar, los datos de carácter personal se definen como toda aquella información personal que pueda conducir a la identificación de un individuo⁸⁵. Además, dentro de los datos personales definidos, hay una categoría de datos que gozan de una mayor protección, bajo la denominación de “categorías particulares de datos” en el art. 6. Estos datos son los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o la vida sexual, y datos de carácter personal referentes a condenas penales⁸⁶. Por otra parte, los datos que se protegen son todos los que reciben un tratamiento automatizado (ya se trate de archivar, clasificar, modificar, enviar a un tercero o suprimir sus datos). Pero también se permite a los Estados extender la protección a datos que no sean objeto de tratamiento automatizado. Una apreciación adicional, es, que el Convenio permite la posibilidad de extraer de su aplicación a categorías enteras de ficheros automatizados de datos de carácter personal, aunque sólo respecto de aquellos datos que su legislación interna excluya del carácter de datos protegidos, según se desprende del art. 3 del Convenio y de su memoria explicativa.

Los principios que establece el Convenio 108 se basan en son dos estándares legales fundamentales: que la información sea correcta, relevante y no excesiva en relación al propósito para el que se obtiene; y que su uso (recogida, almacenamiento y difusión) debe igualmente ser correcto. Un resumen muy acertado de los principios mínimos que subyacen en el Convenio se encuentra en la tesis de Ortega Jiménez, en los siguientes términos:

“a) el Principio del consentimiento, según el cual la finalidad justificativa de la creación de un fichero de datos debe estar definida y predeterminada antes de su puesta en funcionamiento; b) el Principio de lealtad, que implica que la recogida de datos debe realizarse de una forma lícita; c) el Principio de calidad, según el cual el responsable de los datos debe comprobar la exactitud de los datos recopilados y su actualización; d) el Principio de publicidad, que obliga a la existencia de un registro público de los ficheros automatizados; e) el Principio de control, que supone que cualquier persona tiene derecho a conocer si los datos que le conciernen son objeto de tratamiento informatizado y, si así fuera, a obtener copias de ellos, e incluso a su rectificación si fueran erróneos o inexactos; y, f) el Principio de seguridad y confidencialidad en el tratamiento de los

⁸⁵ Consejo de Europa, “Depliant Convention 108”, p.1. Disponible en www.coe.int/dataprotection. Consultado el 1 de julio de 2017.

⁸⁶ Memoria explicativa del convenio 108, *op. cit.*, p. 9, pár. 43-48.

datos, según el cual se debe establecer medidas de seguridad para que los ficheros de datos estén protegidos”⁸⁷.

Además, existe el principio de que los datos deberán conservarse únicamente por el tiempo necesario para cumplir la finalidad para la cual se hayan registrado⁸⁸.

Pero, ¿qué garantías directas ofrece el Convenio a los individuos? El Convenio no es *self-executing*, de manera que del mismo no se derivan derechos individuales⁸⁹. Así, la forma de ejercitar estos derechos se regulará por la legislación interna, ya que el Convenio nada dice al efecto. El Convenio se limita a citar cuatro tipos de derechos: el derecho a conocer la existencia de un fichero de datos, titularidad y fin, el derecho al acceso a los datos del archivo por la persona afectada, el derecho a poder exigir la eliminación o corrección de datos tratados violando las pertinentes normas internas que sean de aplicación de los arts. 5 y 6 (referentes a los principios y a los “datos sensibles”), y el derecho a un recurso pensando en la posibilidad de que cualquiera de los derechos mencionados se viole, pudiendo acudir a la autoridad de protección de datos del país y en su caso, a las autoridades judiciales competentes⁹⁰. En todo caso, las limitaciones a estos derechos únicamente son posibles cuando estén en juego intereses superiores, como la seguridad o la defensa del Estado⁹¹.

Las sanciones contra las violaciones de estos principios materializados en derecho interno, serán establecidas por los Estados (art. 10). Así, el Convenio no proporciona ningún mecanismo internacional para que los sujetos cuyos datos individuales son tratados (particularmente los de países no europeos), puedan acudir a él, con el objetivo de hacer cumplir a sus países las obligaciones impuestas por el Convenio. De esta manera, la mayoría de las Partes y los órganos de la Convención sólo pueden utilizar medios diplomáticos para intentar remediar una violación del Convenio, si se considera que una Parte no lo cumple. Los ciudadanos europeos tienen cierta ventaja en este sentido. Pueden iniciar acciones ante el Tribunal Europeo de Derechos Humanos si un Estado europeo no protege sus derechos a la protección de datos, en particular en virtud del artículo 8 del

⁸⁷ ORTEGA JIMÉNEZ, A., *op.cit.*, p. 49. Consultado el 26 de junio de 2017.

⁸⁸ Consejo de Europa, “Depliant Convention 108”, *op. cit.*, p.1.

⁸⁹ Memoria explicativa del Convenio 108., *op. cit.*, pág. 8, par.39.

⁹⁰ GARZÓN CLARIANA, G., *op.cit.*, p.19

⁹¹ J.-Ph. Walter Chair of the T-PD Deputy Commissioner, Federal Data Protection and Information Commissioner, Switzerland, “The role of Convention 108 in the international cooperation”, 2014, p.2. Disponible en <http://www.coe.int/en/web/data-protection/articles-speeches-and-presentations>. Consultado el 1 de julio de 2017.

Convenio Europeo de Derechos Humanos (esto se analizará con más detalle en apartados posteriores). En este sentido, pueden instar (indirectamente) el cumplimiento del Convenio 108 ante un tribunal internacional. Esto, coloca a los ciudadanos de Estados no europeos que se adhieran a la Convención en una situación de desventaja⁹².

El hecho de que sólo los Estados tengan la facultad de sancionar ante un incumplimiento, junto con la falta de una autoridad internacional de control, no parece que sea la solución más adecuada de cara a la efectividad real del Convenio. Estas características, relacionadas con el seguimiento del Convenio por parte de los Estados, serán uno de los puntos más importantes a tratar en el Protocolo Adicional y en la Modernización del Convenio.

No obstante, es preciso señalar que sí se produjo un cierto desarrollo institucional en el marco del Convenio 108, al crearse el Comité Consultivo (T-PD). Este Comité desempeña un papel central en la aplicación e interpretación del Convenio. La complejidad de las cuestiones relativas a la protección eficaz de los datos personales, provocada en particular por la aparición constante de nuevas tecnologías y prácticas, exige soluciones y análisis innovadores⁹³. El Comité puede hacer propuestas para facilitar o mejorar la aplicación del Convenio, formular propuestas de modificación de la Convención o formular un dictamen sobre cualquier propuesta de enmienda. También puede expresar una opinión a solicitud de una Parte sobre la aplicación de la Convención. Actualmente, permite a más de 60 especialistas de todo el mundo reunirse periódicamente para abordar problemas comunes de protección de datos, proporcionar orientación reglamentaria y conocimientos técnicos sobre algunos aspectos particulares de un sistema nacional y discutir los medios para hacer frente a las dificultades que enfrentan los países en cuestión⁹⁴.

Por último, es necesario hacer referencia a los flujos transfronterizos de datos personales, que será también uno de los aspectos más destacados a la hora de reforzar el Convenio 108 en el Protocolo Adicional y en la Modernización del Convenio. La primera idea es que los Estados parte deberán permitir las exportaciones de datos a los demás Estados Parte de la Convención. La regla general es que los Estados Parte no podrán imponer

⁹² GREENLEAF, G., *op.cit.*, p.8.

⁹³ POLAKIEWICZ, J. *op. cit.*, p. 3

⁹⁴ WALTER, J.-Ph. *op. cit.*, p. 3

obstáculos al flujo de datos transfronterizos mediante prohibiciones o autorizaciones, ya que se considera que todos ellos al transponer el núcleo común del Convenio, tienen un cierto nivel mínimo de protección. En este sentido, el Convenio se refiere únicamente a la exportación de datos y no a su importación. Se considera que la importación no presenta problemas, ya que los datos importados están en todo caso cubiertos por el régimen de protección de datos del Estado importador⁹⁵. Pero el Convenio no dice nada más en relación con los flujos transfronterizos, de manera que presenta algunas lagunas que se intentarán colmar, como veremos, por su Protocolo. Por otra parte, el Convenio establece que las disposiciones que regulan el flujo transfronterizo de datos también se aplican a la recopilación de datos. Ello se consideró necesario para evitar que los datos recogidos en un país y tratados en otro violen las disposiciones del Convenio⁹⁶.

3.3. PROTOCOLO ADICIONAL AL CONVENIO 108 (2001)

El objetivo del Protocolo es aumentar la protección de los datos personales y la privacidad, mejorando el Convenio 108 original fundamentalmente en dos áreas: por un lado, abordando los flujos transfronterizos de datos de carácter personal, llevados a cabo desde un Estado Parte en el Convenio hacia un tercer Estado u Organización Internacional que no lo sea; porque, este supuesto, constituye una laguna expresa en la formulación del art. 12 del Convenio. Por otro lado, creando autoridades nacionales de supervisión, encargadas de velar por el cumplimiento de las leyes o reglamentos adoptados de conformidad con el Convenio, junto con un “*desideratum* un tanto ilusorio, lograr una mejor armonización de los regímenes de control en todo lo relativo a la composición, el funcionamiento y las competencias de las autoridades nacionales de control”⁹⁷.

En cuanto al primer objetivo, el punto de partida es el art. 12 del Convenio 108, que manifiesta cuál debe ser la relación existente entre los flujos transfronterizos de datos de carácter personal y el derecho interno. Pero hay un elemento ausente en la formulación de este artículo en el Convenio 108, y es las restricciones que los Estados Parte deben

⁹⁵ *Ibid.*, p. 10, par.67.

⁹⁶ Memoria explicativa del Convenio 108, *op. cit.*, p. 11, par.64.

⁹⁷ PAVÓN PÉREZ, J.A., “La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales”, *Anuario de la Facultad de Derecho*, N° 19-20, 2001-2002, págs. 235-252, p. 243

hacer a las transferencias de datos a países no signatarios del Convenio. Por lo tanto, se aborda esta laguna debido al gran crecimiento experimentado de los flujos transfronterizos de datos de carácter personal, en concreto, los realizados desde un Estado Parte del Convenio hacia un tercer Estado u Organización Internacional que no lo sea, con niveles de protección absolutamente insuficientes⁹⁸. Y son insuficientes, entre otras cosas, porque al no ser parte en el Convenio 108, no tiene ese núcleo de protección traspuesto a su legislación nacional o a la práctica de la Organización Internacional correspondiente que garantice ese nivel de protección suficiente.

De esta manera, la memoria explicativa del Protocolo justifica que se aborda este aspecto del flujo transfronterizo de datos personales, debido a la globalización de los intercambios internacionales y los progresos de las nuevas tecnologías, lo que supone que se requiere de una mejora constante de la protección efectiva de los derechos garantizados por el Convenio. Y esta mejora en la protección pasa también por cierta armonización internacional de las condiciones en las que se efectúan las transferencias internacionales de datos. En este sentido, el Protocolo, añade un requisito más a estas restricciones, y es, que cada Parte dispondrá que la transferencia de datos de carácter personal hacia un destinatario sometido a la jurisdicción de un Estado u Organización que no sea Parte en el Convenio, sólo podrá efectuarse si dicho Estado u Organización garantiza un nivel de protección adecuado a la transferencia de datos prevista⁹⁹. En otras palabras, los Estados Parte podrán permitir las exportaciones de datos a Estados no Parte, en este caso asegurándose de que los estándares de la Convención para la exportación se cumplan de cara a esos terceros Estados. Así, se establecerán limitaciones a los flujos dirigidos a Estados en que la normativa legal no establece una protección equivalente¹⁰⁰. Ésta es, por lo tanto, esa cierta armonización de condiciones en las que se deben efectuar las transferencias internacionales de datos, en el sentido de tener unos mínimos niveles de protección cuando se realicen. No obstante, estos resultados sólo podrán conseguirse si los órganos de la Convención se aseguran de que los nuevos Estados parte reúnen esos requisitos, y hacen cumplir estos principios. Igualmente es necesario que el resto de

⁹⁸ GUASCH PORTAS, V., *Las transferencias internacionales de datos en la normativa española y comunitaria*, Tesis doctoral, Madrid, 2013, p.75. Disponible en <http://e-spacio.uned.es/fez/eserv/tesisuned:Derecho-Vguasch/Documento.pdf>. Consultado el 15 de julio de 2017.

⁹⁹ Memoria explicativa del Protocolo Adicional al Convenio 108 del Consejo de Europa, sobre autoridades de control y flujo transfronterizo de datos, preámbulo, p.2; Protocolo Adicional al Convenio 108 del Consejo de Europa, sobre autoridades de control y flujo transfronterizo de datos, art. 3.

¹⁰⁰ WALTER, J.-Ph., *op.cit.*, p.2

Estados parte aseguren el cumplimiento de estas directrices, para conseguir un resultado real¹⁰¹.

En cuanto al segundo objetivo, la razón principal de la regulación de las Autoridades de Protección, es, según la memoria explicativa del Protocolo, que el artículo 10 del Convenio 108 exige el establecimiento de recursos y sanciones adecuadas en las disposiciones legales pertinentes de cada Parte, en relación con las violaciones de las normas del derecho interno que transpongan los principios establecidos en el Convenio¹⁰². Sin embargo, el Convenio no obliga a las partes contratantes a establecer mecanismos institucionales que permitan, por ejemplo, la investigación independiente de las quejas, o que supervisen el cumplimiento de los principios en el derecho interno. Por lo tanto, realmente no se garantiza el apoyo y la asistencia a las personas en el ejercicio de sus derechos¹⁰³. Y para ello, el preámbulo del Protocolo adelanta que las Autoridades de Protección son un elemento esencial en la protección efectiva de las personas respecto al tratamiento de datos personales.

De esta manera, el Protocolo establece que cada Parte dispondrá de una o más Autoridades de Protección, que serán responsables de garantizar el cumplimiento de las medidas previstas por su derecho interno que hacen efectivos los principios del Convenio y del Protocolo. Para ello, cualquier persona podrá dirigir a la autoridad de control denuncias o reclamaciones referentes al tratamiento de sus datos personales. También tendrán competencias para la investigación y la intervención. La investigación consiste en la posibilidad de solicitar información relativa al tratamiento de los datos personales y de obtenerlo, haciéndolo accesible en particular, cuando una persona ejerce sus derechos previstos en la normativa nacional. La intervención puede adoptar diversas formas en el derecho interno, por ejemplo, “cuando la autoridad obliga al responsable del fichero a rectificar, borrar o destruir datos inexactos o recolectados ilícitamente; cuando emite medidas cautelares o dictámenes previos a la ejecución de las operaciones de tratamiento de datos; o cuando remite casos a los Parlamentos nacionales u otras instituciones del Estado”¹⁰⁴. También tendrá el poder de iniciar procedimientos legales o de dirigirse a las

¹⁰¹ GREENLEAF, G., *op. cit.*, p.6.,

¹⁰² Memoria explicativa del Protocolo Adicional, *op. cit.*, p.2

¹⁰³ GUASCH PORTAS, V., *op. cit.*, p. 75, 76

¹⁰⁴ SÁNCHEZ GONZÁLEZ, M.A., *Implicaciones institucionales de la ley de protección de datos*, Tesis doctoral, Málaga, 2015, p. 74. Disponible en <https://riuma.uma.es/xmlui/handle/10630/11792>. Consultado el 15 de julio de 2017.

autoridades judiciales correspondientes, en relación con violaciones del derecho interno. Y, además, las decisiones de las autoridades de control que den lugar a reclamaciones podrán ser objeto de recurso jurisdiccional.

3.4. MODERNIZACIÓN DEL CONVENIO (2017)

En 2010 se estimó necesario modernizar el Convenio 108, principalmente para lograr los siguientes objetivos: enfrentar los desafíos derivados de la utilización de las nuevas tecnologías de la información y la comunicación, reforzar la aplicación del Convenio 108 junto con su mecanismo de seguimiento, y abordar la globalización de los flujos transfronterizos de datos personales; todo ello manteniendo su carácter de estándar internacional.

La primera fase de la labor de modernización fue confiada al Comité Consultivo del Convenio 108 (T-PD) y se llegó a un acuerdo sobre las propuestas en su 29ª sesión plenaria de 27-30 de noviembre de 2012. Esas propuestas fueron posteriormente examinadas en 2013 y 2014 por un comité intergubernamental (comité *ad hoc* sobre protección de datos - CAHDATA), que finalizó sus trabajos en una última reunión los días 15 y 16 de junio de 2016¹⁰⁵.

En cuanto a su redacción general, se estableció un consenso claro de que debía mantenerse el carácter general y tecnológicamente neutral de las disposiciones del Convenio 108, preservar la coherencia y la compatibilidad con otros marcos jurídicos pertinentes¹⁰⁶. Es decir, se quería fomentar su carácter de estándar internacional.

El primer desafío ante el que se encuentra la modernización del Convenio 108 es hacer frente a los nuevos retos a la privacidad, abordados en la introducción de este trabajo. Para ello, la modernización está siguiendo, entre otras cosas, los parámetros establecidos en el documento elaborado por el Comité de la Convención 108, denominado *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, de 2017. Este documento tiene como objetivo principal hacer efectivos los

¹⁰⁵Modernisation of Convention 108 (CAHDATA). Disponible en <http://www.coe.int/en/web/data-protection/modernisation-convention108>. Consultado el 15 de junio de 2017.

¹⁰⁶ Memoria explicativa del borrador de la Modernización de la Convención 108, p.1

principios y disposiciones del Convenio 108 en el contexto actual Big Data (que es uno de los principales objetivos del nuevo borrador). Ha sido redactado a la luz del proceso de modernización del Convenio, de manera que está íntimamente ligado con la definitiva conformación del mismo. Está dirigido a los controladores y procesadores de la información, para que puedan tener una guía a la hora de controlar y proteger los datos personales de las personas en este contexto tecnológico, hasta la definitiva aprobación de Convenio 108 en su versión modernizada¹⁰⁷.

En este sentido, las principales novedades que se protegen como consecuencia de estos nuevos retos de privacidad es que los datos personales (definidos en el Convenio 108, como vimos, como cualquier información relativa a un individuo identificado o identificable) adquieren una nueva significación: la protección de los datos anónimos. En principio, los datos anónimos no encajarían en la definición de datos personales ofrecida por el Convenio, porque no deberían permitir la identificación del individuo que ha prestado esos datos, ya que en principio se han obtenido bajo anonimato. Pero debido al avance de la tecnología, ya es posible identificar a los individuos a los que pertenecen tales datos anónimos, por lo que este riesgo de reidentificación adquiere una importancia considerable. Es por ello que la Modernización del Convenio hace hincapié en este punto, ya que ahora, los datos anónimos entrarían dentro de la categoría de datos personales definidos por el Convenio 108. Por otra parte, también se acentúan los peligros que entraña el Big data. Así, por la infinidad de posibilidades que puede ofrecer el tratamiento de datos en masa y los riesgos que conlleva, se debe incitar a los responsables del tratamiento de los datos a considerar la noción de control no solo individualmente, sobre los datos que esté tratando en un momento puntual, sino también de manera preventiva en cuanto al uso y al impacto en la dignidad humana que las técnicas de Big Data puede llegar a suponer, si no se toman las precauciones debidas *ex ante* y *ex post* a su tratamiento¹⁰⁸.

Asimismo, la Modernización el Convenio, también incluye nuevos datos dentro de la “especial categoría de datos”, a los que se refiere el art. 6, que eran aquellos que gozaban de una mayor protección en el Convenio 108, ya que son datos más “sensibles” en el

¹⁰⁷ COUNCIL OF EUROPE, T-PD (2017)01, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasbourg, 2017, p. 1. Disponible en <https://rm.coe.int/16806ebe7a>. Consultado el 1 de mayo de 2017

¹⁰⁸ *Ibid.*, p. 3 y 7

sentido de que se refieren a la zona más íntima de la personalidad. Así, se incluyen, por ejemplo, los datos biométricos o de ADN. Además, se amplía de alguna manera el catálogo de derechos, que incluye, por ejemplo, el derecho a saber por qué un ordenador tomó una decisión sobre cierta persona, como, por ejemplo, la no atribución de un beneficio social, o incluso si esa decisión fue tomada por una máquina altamente sofisticada¹⁰⁹.

Otra de las carencias del Convenio que se ha intentado abordar en su modernización es el mecanismo de seguimiento. Aunque haya una serie de principios que las partes han de adoptar, en realidad no hay ninguna institución específica que se encargue de comprobar que las Partes cumplen sus compromisos¹¹⁰. En esta línea, el borrador mejora las competencias del Comité Consultivo (T-PD) para permitir un mayor seguimiento y evaluación de la Convención en su aplicación por las Partes. De esta forma, el T-PD preparará, antes de cualquier nueva adhesión a la Convención, un dictamen para el Comité de Ministros sobre el nivel de protección de datos del candidato a la adhesión. También, examinará periódicamente la aplicación por las Partes y decidirá las medidas que deberá adoptarse cuando una Parte no esté conforme con la Convención. Asimismo, facilitará, cuando sea necesario, la solución amistosa de todas las dificultades relacionadas con la aplicación del Convenio¹¹¹.

Relacionado con el seguimiento, pero más enfocado en la cooperación entre las Partes, el borrador propone que las Autoridades de Protección de Datos formen una red para el desempeño de sus funciones y se asistan mutuamente¹¹², de manera que dándoles más poder e independencia también se reducirían las interferencias políticas.

Por último, el tercer aspecto fundamental abordado en el borrador es el de los flujos transfronterizos de datos personales, debido a su crecimiento globalizado. El régimen hace hincapié en el aspecto regulado en el Protocolo (transferencias a Estados u Organizaciones Internacionales no parte de la Convención). Tiene por objeto garantizar que los datos personales tratados originalmente en la jurisdicción de una Parte (datos

¹⁰⁹ Secretary General Speech, “Convention 108: from a European reality to a global treaty: Modernising the Convention”, 17 June 2016. Disponible en <http://www.coe.int/en/web/secretary-general/-/convention-108-from-a-european-reality-to-a-global-treaty->. Consultado el 15 de julio de 2017

¹¹⁰ POLAKIEWICZ, J. *op. cit.*, p. 4

¹¹¹ J.-Ph. WALTER, *op. cit.*, p. 6

¹¹² POLAKIEWICZ, J. *op. cit.* p.2 y 5

recopilados o almacenados, por ejemplo), que posteriormente estarán bajo la jurisdicción de un Estado que no es Parte en la Convención, continúen procesándose con las salvaguardias apropiadas¹¹³. Partiendo del principio de libre flujo entre Estados Parte, se distinguen las condiciones de transferencia a países que formen parte de uniones regionales (como la UE), y a terceros países u Organizaciones Internacionales, y cómo se deben evaluar las condiciones de “un nivel adecuado de protección” para realizar las transferencias. Además, se propone que las Autoridades de Protección tengan competencias en ciertos casos, pudiendo requerir al transferente que dé muestra de las garantías apropiadas, o incluso prohibir o suspender ciertas transferencias¹¹⁴.

¹¹³ Memoria explicativa del borrador de la Modernización de la Convención 108, art.12

¹¹⁴ *Ibid*, art.12; Borrador de la Modernización de la Convención 108, art. 12.

IV. LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES: ANTECEDENTES

4.1. INTRODUCCIÓN

Como vimos, dos hitos son destacables en la jurisprudencia del TEDH. La sentencia *Klass and Others c. Alemania*, de 1978, considerada por el TEDH¹¹⁵ como el primer caso en la materia; y el punto de inflexión, en 1997, por ser la fecha de la sentencia¹¹⁶ donde se reconoce expresamente por el Tribunal la existencia autónoma de la protección de datos personales. El TEDH no reconoce, por tanto, la protección de datos personales hasta finales del s. XX. Para llegar a ello, en sus inicios el Tribunal parte del desarrollo del derecho al respeto a la vida privada y familiar, domicilio y correspondencia, consagrado en el art. 8 CEDH; y a medida que van pasando los años y la sociedad evoluciona, y con ella la tecnología; la jurisprudencia del TEDH irá también evolucionando, incorporando al concepto de “vida privada” (ubicado en esta disposición) muy diversos aspectos provenientes de una amplia casuística relativa a los datos personales. Así, en 1997, el Tribunal se refiere expresamente al término protección de datos personales y le atribuye cierta autonomía dentro de la protección otorgada por el derecho al respeto a la vida privada y familiar, domicilio y correspondencia del art. 8 CEDH (en adelante, derecho al respeto a la vida privada).

Estas dos etapas presentan ya, *a priori*, un paralelismo llamativo con los avances tecnológicos. Así, la jurisprudencia durante el s. XX (desde 1978), vendría marcada por la “sociedad de la información”; mientras que la jurisprudencia del Tribunal durante el s. XXI, (de 1997 en adelante) respondería a la “era digital”. Por lo tanto, en el examen de la jurisprudencia del TEDH deben distinguirse dos periodos (s. XX y s. XXI), y ello en íntima conexión con el factor tecnológico.

¹¹⁵ TEDH: *Personal Data*, Factsheet, julio 2017. Disponible en http://www.echr.coe.int/Documents/FS_Data_ENG.pdf. Consultado el 10 de julio de 2017

¹¹⁶ TEDH, *Z. v. Finland*, (nº22009/93), sentencia de 25 de febrero de 1997

Antes de nada, conviene, sin embargo, mencionar algunos datos generales muy significativos que se han identificado en la investigación, y que resultan de interés con el fin de obtener una visión general de la jurisprudencia del TEDH en la materia. Así, partiendo de la distinción entre las dos etapas, en cada una de ellas se identificarán una serie de datos que se refieren a los siguientes aspectos generales. En primer lugar, el número de casos que recibe el Tribunal en las diferentes décadas de los siglos XX y XXI, teniendo en cuenta la jurisprudencia categorizada como referente a “datos personales” y “nuevas tecnologías”¹¹⁷. Ya, mediante el número de casos recibidos, puede hacerse una primera idea de la importancia de la materia (es decir, de la incidencia de la tecnología en la posible vulneración de ciertos derechos fundamentales, y en especial del art. 8 CEDH, que dará lugar a la protección de datos personales). En segundo lugar, podrán apreciarse qué derechos fundamentales se alegan como vulnerados (como se verá, el que más veces aparece es el derecho al respeto de la vida privada y familiar, domicilio y correspondencia –art. 8 CEDH–, que como se ha adelantado, es del que nace el reconocimiento de la protección de los datos personales en la jurisprudencia del TEDH). En tercer lugar, podrá apreciarse cuáles son las áreas de vulneración de esos derechos. Y en cuarto y último lugar, el impacto de las nuevas tecnologías en esa posible vulneración.

En la etapa correspondiente a la sociedad de la información del s. XX, esto es, de 1978 a 1999¹¹⁸ (19 años en total), los datos son los siguientes:

- El Tribunal recibe 2, 4 y 10 casos en cada una de las décadas respectivas (quepa denominar “década” a los años 70, 80 y 90 en general).
- Los derechos que se alegan como vulnerados fundamentalmente son los siguientes. En primer lugar, el derecho al respeto de la vida privada y familiar, domicilio y correspondencia (art. 8 CEDH). Sobre este derecho, aparece un solo caso en la primera década, 4 casos en la segunda, y 8 casos en la tercera. En segundo lugar, el derecho a la libertad de expresión (art. 10 CEDH), que aparece

¹¹⁷Los casos analizados se han obtenido de TEDH: *Personal Data*, Factsheet, julio 2017; TEDH: *Mass Surveillance*, Factsheet, junio 2017; TEDH: *New Technologies*, Factsheet, julio 2017. Disponible en <http://www.echr.coe.int/Pages/home.aspx?p=press/factsheets&c=>. Consultados el 20 de julio de 2017. Y, AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, CONSEJO DE EUROPA, “Manual de legislación europea en materia de la protección de datos”, Belgium, 2014. Disponible en <http://www.coe.int/en/web/data-protection/home>. Consultado el 20 de julio de 2017. Aunque el objeto de análisis sean los casos referentes a la protección de datos, el análisis no se podía limitar únicamente a los casos bajo la rúbrica de “personal data”, ya que los casos recopilados bajo las rúbricas de “new technologies” o “mass surveillance”, contienen numerosos asuntos en los que aparece la protección de los datos personales (además de otros asuntos donde se vulnera la libertad de expresión y otros derechos, que por ello aparecen en las tablas del anexo).

¹¹⁸Estas conclusiones responden a un análisis empírico personal, obtenido de la ordenación de los casos recopilados en función de los criterios recogidos en las tablas situadas en el anexo. La fecha de inicio seleccionada responde a la primera sentencia en la materia (caso *Klass and others*, 1978), según TEDH: *Personal Data*, Factsheet, julio 2017.

en un solo caso en la primera década referido a la libertad de prensa, en un caso en la segunda década (que la Corte reconduce al art. 8 CEDH), y en un caso en la tercera década respecto a la libertad de artes. En tercer lugar, otros derechos también mencionados de manera más aislada: el derecho a un recurso efectivo ante una instancia nacional (art. 13 CEDH), que sólo consta un caso en la segunda década, acompañando al art. 8, y en un caso en la tercera década, también acompañando al art. 8; y el derecho a un proceso equitativo (art. 6 CEDH), que sólo aparece una vez en la segunda década, y una vez en la tercera.

- Las áreas de vulneración de los derechos son limitadas. En la primera década, resaltan la vigilancia masiva y recogida de datos (normalmente mediante interceptación de comunicaciones telefónicas, correspondencia o vigilancia secreta). En la segunda década, aparece como nuevas áreas de vulneración el almacenamiento de datos (en registros secretos) y uso de esos datos, y la denegación del acceso a datos que han sido almacenados. En la tercera década, aparecen finalmente el almacenamiento y uso de datos (referentes a la salud) y la divulgación de datos personales.
- Durante estos años se produce una transición de la tecnología propia de la sociedad de la información (que como se explicó en anteriores apartados, nació aproximadamente en los años 60), a la tecnología propia de la era digital. Por lo tanto, puede apreciarse que a medida que la sociedad va evolucionando y la tecnología con ella, existe una incidencia tecnológica en la vulneración de los derechos que es creciente, y se aprecia, sobre todo, en la interceptación de las comunicaciones del momento; es decir, correspondencia, luego teléfono, etc.¹¹⁹ Es una etapa donde la incidencia tecnológica se caracteriza por conllevar un conflicto de intereses, entre los del particular y los del Estado, fundamentalmente.

En la era digital del s. XXI, esto es, de 2000 a 2017 (17 años aproximadamente), cabe destacar lo siguiente:

- El TEDH recibe alrededor de 46 casos en la primera década (de 2000 a 2009), y desde entonces hasta la actualidad, conoce alrededor de 78 casos. Este dato es muy significativo, ya que la primera década del s. XXI supone multiplicar por

¹¹⁹ Para ver cuáles son las principales sentencias con estas características, ver Anexo 2. La Jurisprudencia del TEDH en materia de protección de datos: orden cronológico

cuatro el número de casos que recibe el Tribunal con respecto a la última década del s. XX. Y en la segunda década del s. XXI, aún no terminada, la Corte ha recibido un récord histórico de casos en la materia.

- Entre los derechos que se alegan como vulnerados aparece fundamentalmente el derecho a la vida privada y familiar (art.8) en 34 casos en la primera década, y en 52 casos en lo que llevamos de segunda década; al que ocasionalmente acompaña el derecho a un recurso efectivo ante una instancia nacional (art. 13 CEDH), en 3 y 4 casos respectivamente. En segundo lugar, el derecho a la libertad de expresión (art. 10 CEDH), aparece en 7 casos en la primera década, y en 20 casos en lo que llevamos de segunda década; mediante su manifestación en publicaciones en internet, publicación de fotografías en prensa, y acceso a la información en general. Cabe apreciar que estos derechos se alegan separadamente, alegando bien la vulneración de la libertad de expresión, bien la vulneración de la vida privada y familiar en la primera década, y que coexisten aisladamente en algunos casos en lo que llevamos de segunda década. Por otra parte, aparecen también el derecho a la propiedad (Protocolo Adicional al CEDH nº 1) en un caso en la primera década y otro caso en lo que llevamos de segunda; el derecho a un proceso equitativo (art. 6 CEDH) en 2 casos en la primera década y 3 casos en lo que llevamos segunda. Finalmente, aparecen también otros derechos de manera más aislada: el derecho al respeto de los derechos humanos (art.1 CEDH) en un único caso en la primera década, el derecho a la libertad y la seguridad (art.5 CEDH) en un único caso en lo que llevamos de segunda década, y prohibición de pena sin ley (art.7) también en un único caso en lo que llevamos de segunda década.
- Las áreas de vulneración del derecho crecen notablemente en la primera década. Aparte de las mencionadas, aparecen nuevas áreas de vulneración, tanto dentro de las existentes (en almacenamiento y uso, ahora también en el contexto de la justicia penal; en interceptación de las comunicaciones, ahora también la monitorización de los ordenadores de los empleados o muestras de voz), como nuevos tipos (eliminación o destrucción de datos, varios métodos de vigilancia, imágenes, internet, email, datos electrónicos, o antenas parabólicas). En lo que llevamos de segunda década, las áreas de vulneración del derecho vuelven a crecer, algunas dentro de las ya conocidas (en recogida de datos, el uso del GPS; en almacenamiento y uso, en procedimientos de seguros sociales y proveedores de servicios de telecomunicaciones) y otras áreas nuevas (como

radiocomunicaciones, identidad, uso de cámaras ocultas, telecomunicaciones, o derechos de autor musicales “*copyright*”).

- El impacto de la tecnología en la era digital marca esta etapa: aparecen casos en los que el uso de las nuevas tecnologías y la evolución de la informática tienen un papel fundamental. El reflejo de esta circunstancia en la jurisprudencia del Tribunal es también una situación innegable. Sin embargo, cabe resaltar que sigue teniendo mucho protagonismo en la vulneración de los derechos la tecnología propia del s. XX (interceptación de conversaciones telefónicas, vigilancia, imágenes, etc.), y, curiosamente, no se encuentran apenas casos referentes a la ciencia más puntera que en teoría supone un mayor peligro a la protección de los datos personales: hablamos del Big Data en general, y las transferencias ilícitas internacionales de datos, caracterizadas por tener un marcado carácter económico. Esta apreciación será objeto de desarrollo en un apartado posterior, dedicado al análisis de los casos donde las tecnologías del s. XXI están más presentes, para poder concluir de manera más acertada la traslación y el impacto real de las ciencias más punteras en la vulneración de los derechos, y especialmente, en la protección de los datos personales¹²⁰.

4.2. ANTECEDENTES DE LA PROTECCIÓN DE DATOS PERSONALES: LA JURISPRUDENCIA SOBRE EL DERECHO AL RESPETO A LA VIDA PRIVADA Y FAMILIAR, DOMICILIO Y CORRESPONDENCIA (ART. 8 CEDH) DURANTE EL S. XX (DE 1978 A 1997)

4.2.1. Tratamiento general: contenido del derecho y principios

En la jurisprudencia analizada correspondiente al s. XX, en el periodo comprendido entre 1970 hasta 1997, es posible identificar algunas sentencias que, si bien giran fundamentalmente entorno al art. 8 CEDH, van contribuyendo a conformar el contenido del derecho a la protección de datos personales.

Debe recordarse que el art. 8 CEDH proclama el derecho a la vida privada y familiar,

¹²⁰ Para ver cuáles son las principales sentencias con estas características, ver Anexo 2. La Jurisprudencia del TEDH en materia de protección de datos: orden cronológico

domicilio y correspondencia. Los bienes jurídicos protegidos –vida privada, familia, domicilio y correspondencia– tienen una estrecha relación entre sí, ya que todos conducen al mismo objetivo de proteger una esfera de actuación y de desarrollo personal autónoma. Pero en realidad, los dos últimos son diversos aspectos que se incluyen dentro del bien jurídico más general de vida privada. Pero son mencionados expresamente porque son más concretos, y porque pueden ser violados de manera más autónoma, sin atentar en todos los casos contra aspectos realmente reservados o íntimos de la persona¹²¹.

En algunos de los casos examinados¹²² se consideran simultáneamente varios de los bienes jurídicos protegidos por el art. 8 CEDH (vida privada y correspondencia, por ejemplo) sin necesidad de delimitar sus ámbitos. Porque realmente, ante cualquier injerencia en la esfera personal, puede invocarse sin mayor precisión la vulneración del art. 8.1 en su conjunto¹²³.

Pero además del contenido del derecho que se corresponde con la literalidad de su enunciación en el art. 8 CEDH, durante el s. XX, la interpretación del bien jurídico protegido va siendo ampliada, de manera que el Tribunal va estableciendo como parte de la vida privada los siguientes aspectos¹²⁴: la información que pueda obtenerse de la interceptación de las comunicaciones en general y entre ellas conversaciones telefónicas (aparte de la correspondencia), la información sobre la actividad sindical, la información sobre la vida profesional y laboral, e incluso la información sobre los propios orígenes e identidad. Todo ello forma parte del contenido del derecho al respeto de la vida privada y familiar, domicilio y correspondencia (art. 8 CEDH).

El contenido del derecho que va formulando el Tribunal es, por tanto, bastante amplio, amoldándose a diferentes casuísticas y formas de vulneración, y donde las tecnologías de la época (sobre todo las referentes a las comunicaciones) inciden bastante en las injerencias perpetradas en el ejercicio del derecho. Así, el desarrollo en el contenido del derecho que se va conformando durante estos años incidirá en el contenido que

¹²¹ ARZOZ SANTISTEBAN, X., “Derecho al respeto de la vida privada y familiar” en ARZOZ SANTISTEBAN, X., *Convenio Europeo de Derechos Humanos: Comentario sistemático*, Estudios y Comentarios Legislativos (Civitas). Editorial Aranzadi, S.A.U., Enero de 2009, p. 1-11, p. 10

¹²² Por ejemplo, TEDH, *Silver and Others v. United Kingdom* (nº7136/35), sentencia de 25 de marzo de 1983

¹²³ ARZOZ SANTISTEBAN, X., “Derecho al respeto de la vida privada y familiar” en ARZOZ SANTISTEBAN, X., *Convenio Europeo de Derechos Humanos: Comentario sistemático*, Estudios y Comentarios Legislativos (Civitas). Editorial Aranzadi, S.A.U., Enero de 2009, p. 1-11, p. 10

¹²⁴ Respectivamente, sentencias TEDH, *Klass and Others v. Germany*, (nº5029/7), sentencia de 6 de septiembre de 1978; TEDH, *Malone v. the United Kingdom*, (nº8691/79), sentencia de 2 de agosto de 1984; TEDH, *Kruslin v. France* (nº11801/85), sentencia de 24 de abril de 1990; TEDH, *Silver and Others v. United Kingdom* (nº7136/35), sentencia de 25 de marzo de 1983; TEDH, *Leander v. Sweden* (nº9248/81), sentencia de 26 de marzo de 1987; TEDH, *Niemietz v. Germany* (nº13710/88), sentencia de 16 de diciembre de 1992; TEDH, *Gaskin v. the United Kingdom*, (nº10454/83), sentencia de 7 de julio de 1989

posteriormente tendrá la protección de datos personales en la jurisprudencia del TEDH, en la medida en que está inserta igualmente en el concepto de “vida privada y familiar”. Por tanto, muchos de estos desarrollos aparecerán también en la jurisprudencia del s. XXI, pero ya no simplemente dentro del concepto vida privada, sino también dentro del área autónoma de protección de los datos personales, que, a su vez, se insertará en el concepto de vida privada.

El art. 8, al reconocer literalmente el derecho al respeto a la vida privada y familiar, domicilio y correspondencia, permite a los Estados regular con cierta libertad este derecho. Esto supone que hay injerencias que no constituyen una vulneración del mismo. Además, este derecho no es un derecho absoluto, sino que debe ser ponderado con otros intereses públicos o privados, antes de decidir si la injerencia supone o no una vulneración del derecho.

De esta manera, para establecer si ha habido o no vulneración del art. 8 CEDH, el Tribunal ha seguido fundamentalmente el *principio de tratamiento lícito de los datos o de injerencia justificada*, que se ha advertido a lo largo de su jurisprudencia durante todo el s. XX. Así, en primer lugar, el Tribunal procede a determinar si se ha producido la injerencia en el derecho al respeto a la vida privada y familiar, de su domicilio o de su correspondencia. El objetivo es concluir si ha habido una vulneración del bien jurídico protegido, no enjuiciar la licitud de la medida¹²⁵. Como se ha visto en el apartado anterior, el bien jurídico protegido que va conformando el Tribunal va adoptando un contenido muy amplio.

En segundo lugar, el Tribunal procede a analizar si dicha intromisión se haya prevista por ley, y si es legítima, de conformidad con el art. 8.2. El objetivo aquí es, por tanto, un juicio de legalidad de la medida, para comprobar si la injerencia está respaldada por el Derecho. Además, la ley debe ser accesible a los interesados y previsible en cuanto a sus efectos. Esto quiere decir que las personas a las que concierne determinada norma, puedan acceder a ella fácilmente, y así, puedan conducir su comportamiento y conducta de acuerdo con lo que disponga. También el Tribunal examina su legitimidad, con el fin de determinar si persigue alguno de los objetivos enunciados en el art. 8.2, es decir: seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del

¹²⁵ MARTINEZ MARTINEZ, R., *op.cit.*, p. 162

orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

El tercer paso es analizar la intromisión bajo un juicio de proporcionalidad o necesidad: es decir, que la injerencia responda a una necesidad social fundamental, imperiosa o acuciante, en una sociedad democrática; y que sea proporcional al objetivo o fin legítimo perseguido. De entre las necesidades proclamadas por el artículo, en la mayoría de los casos respondían a la prevención del delito o de seguridad nacional. No obstante, el requisito de necesidad va siendo interpretado de manera flexible y según el país y sus circunstancias, no exigiendo las mismas características en cada caso, sino estudiándolo en su contexto¹²⁶.

Cabe apreciar que este principio de tratamiento lícito de los datos o de injerencia justificada y todos los pasos que conlleva para vislumbrar si ha habido vulneración del art. 8 CEDH, se constituye como antecedente¹²⁷ del tratamiento que el Tribunal proporcionará a la protección de los datos personales, cuando esta área sea reconocida expresamente a finales del s. XX, y durante el s. XXI. Ya que, como la protección de datos personales se incardina dentro del art. 8 CEDH, este principio será igualmente aplicado, para apreciar por parte del Tribunal si ha habido una vulneración del art. 8, y en especial, con respecto al área de protección de los datos personales.

4.2.2. Relación con otros derechos

El derecho a la vida privada y familiar, domicilio y correspondencia, no es un derecho absoluto. Y, tal como establece el art. 8.2, es posible permitir una injerencia en el ejercicio de este derecho en la medida en que “esté prevista por la ley y sea necesaria en una sociedad democrática para (...) la protección de los derechos y libertades fundamentales de los demás”. En este sentido, durante el examen de la jurisprudencia, ha podido comprobarse que algunas injerencias en el ejercicio del derecho al respeto de la vida privada y familiar, pueden permitirse y estar justificadas en aras de la protección y el

¹²⁶ *Ibid*, p.164

¹²⁷ Por ejemplo, TEDH, *Klass and Others v. Germany*, (nº5029/7), sentencia de 6 de septiembre de 1978; TEDH, *Malone v. the United Kingdom*, (nº8691/79), sentencia de 2 de agosto de 1984; TEDH, *Leander v. Sweden* (nº9248/81), sentencia de 26 de marzo de 1987; TEDH, *Silver and Others v. United Kingdom* (nº7136/35), sentencia de 25 de marzo de 1983; TEDH, *The Sunday Times v. the United Kingdom*, (nº6538/74), sentencia de 26 de abril de 1979

ejercicio efectivo de otros derechos.

No obstante, en la jurisprudencia analizada desde 1970 a 1997, sólo se han advertido dos casos¹²⁸ donde aparece alegado un derecho diferente: la libertad de expresión del art. 10 CEDH, aunque no hay realmente una pugna de derechos entre la libertad de expresión y el respeto a la vida privada y familiar.

Como veremos, será en el apartado correspondiente a la jurisprudencia entre 1997 a 2017 donde aparecerán realmente los derechos que entran en conflicto o que el Tribunal pondera con respecto al art. 8 CEDH.

4.2.3. Acciones de las personas

Los individuos deben estar facultados por la legislación nacional para hacer efectivo el derecho al respeto a la vida privada y familiar, mediante diversos mecanismos o derechos que el Estado en cuestión ponga a su disposición. Estos mecanismos son variados, y se deben situar en diversos momentos, para garantizar una protección efectiva. Es decir, en primer lugar, es necesario un mecanismo situado en un momento o fase preventiva, que en general permita al individuo, entre otras cosas, elegir qué ámbito de su esfera privada puede ser conocido por terceros, o que le permita conocer qué ámbitos de su vida privada está en manos de otras personas u organismos públicos. Y, en segundo lugar, es necesario un mecanismo situado en una fase o momento posterior a la vulneración, que, de alguna manera, permita el resarcimiento o la paralización de dicha vulneración a su derecho.

No obstante, la mayoría de estos mecanismos han sido consolidados y desarrollados en la jurisprudencia del s. XXI, tras el reconocimiento expreso de la protección de los datos personales dentro del art. 8 CEDH. Sin embargo, durante el s. XX, destacan dos casos que tienen una gran trascendencia. Por un lado, porque supondrán el punto de partida para la consolidación en el s. XXI de algunos de estos mecanismos de tutela en cuanto a la protección de datos personales, y, por otro lado, porque se configuran como antecedentes directos, suponiendo un paso esencial para el reconocimiento en sí de la materia que nos

¹²⁸ TEDH, *The Sunday Times v. the United Kingdom*, (nº6538/74), sentencia de 26 de abril de 1979; TEDH, *Silver and Others v. United Kingdom* (nº7136/35), sentencia de 25 de marzo de 1983

ocupa.

En primer lugar, llama la atención el caso *Leander c. Suecia*, de 1987. En este caso, se verifica la posible vulneración del derecho a la vida privada y familiar, por el rechazo de la rectificación o cancelación de unos informes que contenían información del interesado referente a sus ideales políticos y sindicales. Así, en el pár. 48 de la sentencia del TEDH, se señala por primera vez la relación entre datos de carácter personal y el derecho a la vida privada. El Tribunal establece que el almacenamiento y uso de esa información, junto con la negación de ese posible derecho a la rectificación o cancelación de los informes ostentados por la policía, constituyen un atentado contra el derecho del art. 8 CEDH. Sin embargo, todavía no es el caso definitivo en el que se reconoce de manera expresa la protección de los datos personales, porque el Tribunal, no habla en términos de dato personal, sino que sigue hablando en términos de información referente a la vida privada¹²⁹. Pero es un antecedente muy importante.

El segundo caso es el de *Gaskin c. Reino Unido*, de 1989. En este asunto, el interesado desea acceder a unos expedientes que recogen ciertos hechos referentes a su pasado, en particular, sobre su infancia y adolescencia en diversos centros de acogida, porque alega haber sufrido malos tratos durante ese periodo. Es decir, lo importante, como se adelantó anteriormente, es la posible existencia de un derecho de acceso a los datos personales que se contienen en esos expedientes. Sin embargo, el Tribunal evita pronunciarse sobre este aspecto, y simplemente considera que esa información entra dentro del ámbito protegido por el derecho a la vida privada y familiar, de manera que se inclina por verificar si ha existido la clásica injerencia en el derecho y su licitud, legitimidad, necesidad y proporcionalidad, y la existencia de obligaciones positivas para el Estado, como se verá a continuación.

4.2.4. Obligaciones de los Estados

Del CEDH dimanaban una serie de obligaciones dirigidas a los Estados Parte, para hacer efectivos los derechos que se consagran en el Convenio. Generalmente, la interpretación clásica de los derechos consagrados en el CEDH comporta obligaciones

¹²⁹ *Op cit.*, MARTÍNEZ MARTÍNEZ, R., p. 196

fundamentalmente negativas. Es decir, que los Estados están obligados a abstenerse de cometer injerencias, en este caso, en el ejercicio del derecho al respeto de la vida privada y familiar, domicilio y correspondencia, excepto en los casos previstos por el art.8.2 CEDH¹³⁰. En este sentido se constatan la mayoría de las obligaciones de los Estados. El Tribunal, mediante los principios anteriormente explicados, examina si el Estado ha cumplido esta obligación de no injerencia arbitraria de los poderes públicos en el ejercicio del derecho, o si, por el contrario, el incumplimiento de la obligación era lícito, legítimo, proporcional y necesario¹³¹. Esta jurisprudencia, ya consolidada en esta fase, se reproducirá en las sentencias adoptadas por el TEDH en el s. XXI, aunque también habrá muchos otros aspectos novedosos, como veremos.

En esta primera fase, también ha habido casos en los que el Tribunal ha establecido que las obligaciones del Estado no consisten solamente en abstenerse de realizar otras injerencias parecidas, sino que también tiene otras obligaciones positivas inherentes a un respeto efectivo de la vida privada y familiar. Porque, además, la injerencia puede provenir no sólo de un acto del Estado, sino también de una omisión. El antecedente más importante en este ámbito es el caso *Gaskin c. Reino Unido*, de 1989.

Es decir, a veces, llegan casos al Tribunal que no tratan tanto de la existencia o no de una injerencia por parte del Estado en la vida privada y familiar, sino que se centran en la cuestión de si el respeto efectivo de este derecho impone una determinada acción del Estado, que conlleve el mejoramiento del *status* de ciertas personas o de eliminación de ciertas trabas. Hablamos, por tanto, de obligaciones positivas, como aquellas acciones del Estado en sentido amplio, que supongan satisfacer los intereses del individuo en cuanto a la esfera del respeto a su vida privada y familiar, para garantizar el ejercicio efectivo de su derecho. Algunos ejemplos pueden ser, como en el caso *Gaskin c. Reino Unido*, permitir o no a una persona conocer el expediente personal que durante su infancia fue elaborado por los servicios sociales; o, por ejemplo, hasta qué punto debe llegar la protección que deben otorgar los poderes públicos frente a las injerencias en el derecho

¹³⁰ PETTITTI, L.-E.: *La convention européenne des droits de l'Homme*, Económica, Paris, 1999, p. 305-320.

¹³¹ Las obligaciones negativas, básicamente se refieren a la no injerencia arbitraria en el ejercicio del derecho. Por ello, para ver ejemplos de las obligaciones estatales, pueden consultarse en la tabla del anexo referente a los principios de tratamiento, es decir, en Anexo 5. La Jurisprudencia del TEDH en materia de protección de datos: principios en el tratamiento del derecho por parte del Tribunal

provenientes de terceros¹³². Además, el Tribunal, ya de conformidad con la jurisprudencia consolidada con respecto a las obligaciones positivas de los Estados, al determinar si existe o no tal obligación positiva, tendrá en cuenta el justo equilibrio que debe alcanzarse entre el interés general de la comunidad y los intereses de la persona.

La sentencia en el asunto *Gaskin c. Reino Unido* se configura como un antecedente muy importante de la protección de datos personales. Porque, cuando el Tribunal reconozca la protección de los datos personales como un área autónoma de protección dentro del art. 8 CEDH, estas obligaciones positivas del Estado que garantizan el ejercicio efectivo del derecho al respeto a la vida privada, también aparecerán durante la jurisprudencia del s. XXI, para la efectiva protección de los datos personales. Y no sólo eso, sino que también contribuirá al reconocimiento expreso de la materia por el Tribunal. Porque, como se ha adelantado, en este caso, el hecho de que se haga hincapié en la cuestión de la obligación positiva del Estado con respecto a la garantía del derecho consagrado en el art. 8 CEDH, es una forma de evitar el problema que late en el fondo, que es la existencia de un derecho de acceso a los datos personales¹³³, que se deriva a su vez de un área autónoma de protección dentro del art. 8 CEDH, que es la protección de datos personales. Pero el Tribunal evita pronunciarse sobre ello, reconduciendo la cuestión a las obligaciones positivas del Estado en garantía del genérico derecho al respeto a la vida privada y familiar.

¹³² ARZOZ SANTISTEBAN, X., "Derecho al respeto de la vida privada y familiar" en ARZOZ SANTISTEBAN, X., *Convenio Europeo de Derechos Humanos: Comentario sistemático*, Estudios y Comentarios Legislativos (Civitas). Editorial Aranzadi, S.A.U., Enero de 2009, p. 1-11, p. 10

¹³³ *Op cit.*, MARTÍNEZ MARTÍNEZ, R., p. 198

V. LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES: RECONOCIMIENTO Y DESARROLLO

El punto de inflexión en la materia viene marcado por el reconocimiento expreso por parte del Tribunal del derecho a la protección de datos personales, en su sentencia de 1997 en el caso *Z c. Finlandia*, aunque, siempre, dentro del marco del derecho consagrado en el art. 8 CEDH. A partir de ese momento, se produce un enorme desarrollo de este derecho en la jurisprudencia del TEDH, en los términos que se verán. Pero, antes de nada, resulta necesario detenerse en el caso *Z. c Finlandia*.

5.1. RECONOCIMIENTO DE LA PROTECCIÓN DE DATOS PERSONALES: CASO Z. C. FINLANDIA, DE 1997.

En este caso, el TEDH reconoce por fin la protección de los datos personales como tal, si bien, como elemento integrado en el derecho al respeto de la vida privada y familiar del art. 8 CEDH¹³⁴, pero con entidad propia. Lo hace desde la perspectiva de entender los datos médicos (en especial la infección de una persona por VIH) como datos personales, y ello aplicando la Recomendación (89) 14 del Consejo de Europa sobre las incidencias éticas de la infección por VIH en el marco sanitario y social¹³⁵. En el caso, estos datos fueron usados por los poderes del Estado en el contexto de un proceso judicial, mediante el mandato de revelarlos dirigido a los médicos, en contra de la voluntad de la demandante. Además, estos datos fueron revelados a un público mayor, mediante la publicación de la sentencia. Así, en el caso, se verifica si los testimonios de los médicos en el juicio y la difusión del fallo, supusieron una injerencia en el derecho al respeto de la vida privada y familiar.

De esta manera, el Tribunal reconoce que la protección de los datos personales (y no sólo los médicos) son de fundamental importancia para que una persona pueda ejercer su derecho al respeto de la vida privada y familiar, tal y como se garantiza en el art. 8 CEDH.

¹³⁴ MARTÍNEZ MARTÍNEZ, R., *op.cit.*, p. 199

¹³⁵ CONSEJO DE EUROPA, Comité de Ministros, Recommendation (89)14 sur les incidences éthiques de l'infection VIH dans le cadre sanitaire et social, Doc. CM/Rec(89)14, de 24 de octubre de 1989

De esta manera, el Tribunal se aproxima a la protección de datos personales (en el caso, datos médicos) como un elemento integrado en el derecho al respeto a la vida privada y familiar (art. 8 CEDH)¹³⁶.

En diversos casos sucesivos, el TEDH va perfeccionando y reafirmando esta primera interpretación jurisprudencial. Así, en primer lugar, el Tribunal vuelve a realizar esta afirmación en el caso *M.S. c. Suecia*, en 1997, también en el marco del tratamiento de datos médicos. La repite asimismo en el caso *Amman c. Suiza*, del año 2000, esta vez referido a datos relativos a la vida profesional.

Por lo tanto, la construcción jurisprudencial de la protección de datos personales se conforma como un área dentro del bien jurídico extraordinariamente amplio del derecho al respeto a la vida privada y familiar, domicilio y correspondencia, que se fue construyendo a lo largo del s. XX. Y por ello, la forma en la que el Tribunal abordará los casos sobre la materia, como antes se ha adelantado, será fundamentalmente de la misma manera en que ha abordado los casos en los que se discutía la vulneración o no del art. 8 antes del reconocimiento de la protección de datos como tal, con algunas novedades propias de su desarrollo.

Un dato también importante es que la aparición en la jurisprudencia del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter Personal de 1981, es simultánea al reconocimiento de la protección de datos personales. Y esta presencia traerá consigo varios aspectos que se analizarán a continuación.

¹³⁶ TEDH, *Z. v. Finland*, (nº 22009/93), sentencia de 25 de febrero de 1997, para. 45

5.2. DESARROLLO DE LA PROTECCIÓN DE DATOS PERSONALES: LA JURISPRUDENCIA SOBRE EL DERECHO AL RESPETO A LA VIDA PRIVADA Y FAMILIAR, DOMICILIO Y CORRESPONDENCIA (ART. 8 CEDH) DURANTE EL S. XXI (DE 1997 A 2017)

5.2.1. Tratamiento general: contenido del derecho y principios

Como se ha explicado, en los casos *Z. c. Finlandia*, *M.S. c. Suecia* y *Amman c. Suiza*, el Tribunal ya se aproxima a la protección de datos personales como un elemento integrado, pero a la vez separado, en el derecho al respeto a la vida privada y familiar (art. 8 CEDH); aunque en este último caso, el Tribunal hace una afirmación sobre el contenido de la protección de datos personales realmente importante, y es la siguiente.

Establece que las diversas operaciones (como se ha visto en los casos anteriores, por ejemplo, comunicación, almacenamiento, uso, divulgación, etc.) que se puedan realizar con datos referentes a la vida privada quedan cubiertas por la protección del art. 8 CEDH, consolidándose la amplísima interpretación que se le ha ido confiriendo al término “vida privada” a lo largo de su jurisprudencia. Establece además que esa amplia interpretación del término “vida privada” se corresponde con la interpretación que realiza el Convenio 108 en lo que respecta al tratamiento automatizado de datos de carácter personal, cuyo objetivo es "asegurar en el territorio de cada Estado Parte, para cada individuo (...) el respeto de sus derechos y libertades fundamentales, y en particular su derecho a la intimidad, en lo que se refiere al tratamiento automatizado de los datos personales que le conciernen"(art.1), y que define tales datos personales como “cualquier información referente a un individuo identificado o identificable” (art.2).

Finalmente, en el caso *Rotaru c. Rumania*, del año 2000, el TEDH consolida esta importante interpretación jurisprudencial sobre la protección de los datos personales¹³⁷, que puede explicarse de la siguiente manera. Por un lado, el reconocimiento del tratamiento de los datos personales como parte del bien jurídico protegido por el art. 8 del CEDH; y por otro, la interpretación amplia del término “vida privada” (que posibilita la primera afirmación), ya que su interpretación se corresponde con la elaboración jurisprudencial del art. 8 CEDH y con la definición contenida en el Convenio 108.

¹³⁷ *Op. cit.*, MARTÍNEZ MARTÍNEZ, R., p. 203

Por lo tanto, el término que se utiliza en este trabajo para hacer referencia a la materia objeto de investigación, “protección de datos personales”, para el Tribunal es, en resumen, la protección ante el tratamiento (es decir, diversas operaciones como almacenamiento, uso, comunicación, divulgación, etc.) de los datos con contenido referente a la vida privada (entendiendo por vida privada la casuística jurisprudencial que ha quedado inserta en el término, durante todo el s. XX –abriendo la puerta a la sucesiva casuística que también se podrá insertar durante el s. XXI¹³⁸- y la definición contenida en el Convenio 108).

En la jurisprudencia analizada durante el s. XXI, hay varias sentencias¹³⁹ que establecen como parte de la vida privada tutelada por el art. 8 CEDH los siguientes aspectos: la vida profesional, la información obtenida por grabaciones de voz, la videovigilancia, los perfiles de ADN junto con muestras celulares y huellas dactilares, la información de tipo geográfica vertida por un GPS, la información referente a los orígenes de una persona o a su identidad, y fotografías o imágenes.

Todo este desarrollo jurisprudencial (incluido el del s. XX) nos permite definir el contenido de los datos personales protegidos por el art. 8 CEDH de la siguiente manera. Así, son datos que se refieren, en primer lugar, a las personas. Serán datos personales aquellos que estén relacionados a una persona identificada o identificable. Es decir, información que identifica a un individuo, o una descripción que haga posible identificar al individuo en cuestión. Se refiere, por tanto, principalmente a personas físicas. En algunos casos el Tribunal ha llegado a conocer de demandas de personas jurídicas¹⁴⁰, pero la protección de la vida privada y familiar por el artículo 8 del CEDH no parece aplicable a las personas jurídicas. Ello no quiere decir que las personas jurídicas no estén protegidas por dicho artículo, sino “por otros derechos contenidos en el artículo 8 del CEDH, como

¹³⁸ En este sentido, el Tribunal ha establecido que “el término vida privada y familiar contenido en el art. 8 CEDH, no es susceptible de definición exhaustiva”. SANTOLAYA MACHETTI, P., *La Europa de los Derechos: El Convenio Europeo de Derechos Humanos*, Centro de Estudios Políticos y Constitucionales, Madrid, 2005, p.547. De esta manera, según la casuística, el TEDH ha ido incorporando a lo largo de los años diversos aspectos que según su criterio entraban dentro del término de vida privada y familiar, sin cerrarse a una definición acotada.

¹³⁹ TEDH, *Amann v. Switzerland* [GC], (nº27798/95), sentencia de 16 de febrero de 2000; TEDH, *Rotaru v. Romania* [GC], (nº28341/95), sentencia de 4 de mayo de 2000; TEDH, *P.G. and J.H. v. the United Kingdom*, (nº44787/98), de 25 de septiembre de 2001; TEDH, *Wisse v. France*, (nº 71611/01), sentencia de 20 de diciembre de 2005; TEDH, *Peck v. the United Kingdom*, (nº44647/98), sentencia de 28 de enero de 2003; TEDH, *S. and Marper v. the United Kingdom*, (nº30562/04 and 30566/04), sentencia de 4 de diciembre de 2008; TEDH, *Uzun v. Germany*, (nº35623/05), sentencia de 2 de septiembre de 2010; TEDH, *Godelli v. Italy*, (nº33783/09), sentencia de 25 de septiembre de 2012; TEDH, *Sciacca v. Italy*, (nº50774/99), sentencia de 11 de enero de 2005; TEDH, *Von Hannover v. Germany*, (nº59320/00), sentencia de 24 de junio de 2004

¹⁴⁰ TEDH, *Bernh Larsen Holding AS and Others v. Norway*, (nº24117/08), sentencia de 14 de marzo de 2013; TEDH, *Liberty and Others v. the United Kingdom*, (nº58243/00), sentencia de 1 de julio de 2008

la inviolabilidad del domicilio y la correspondencia”¹⁴¹. Esta última afirmación se aplicaría también, por tanto, para los datos “personales” referentes a las personas jurídicas, es decir, que tendrían este otro cauce de protección.

Los aspectos que caben dentro del concepto vida privada, (y, por tanto, los diferentes tipos de datos personales) puede apreciarse que son de diversa naturaleza, mientras se refieran a una persona. Estos datos podrán referirse a la mayor parte de las manifestaciones de la personalidad y su desarrollo, con aspectos de la identidad, del reducido ámbito familiar, pero también referentes a sus relaciones con otros seres humanos, incluyendo el ámbito profesional, comercial, social, y de la vida pública de una persona¹⁴². Así, protege elementos muy diversos a los que pueda hacer referencia, como la integridad física y psicológica, el género, nombre, orientación sexual, historia familiar, etnia, datos médicos... Del mismo modo, abarca toda la información sobre un individuo, de manera directa, pero también información que indirectamente revele datos de una persona, por ejemplo, la relación que pueda haber entre un individuo y un evento o un objeto (caso paradigmático, localización que marca el GPS en el caso *Marper*).

Y, por último, cabe destacar que la forma en que la información se materializa es también diversa. Ya sea mediante sonidos, conversaciones, por escrito, imágenes, vídeos, en papel o almacenada electrónicamente, mediante automatización de datos informáticos, ya literales o anónimos, mediante datos biométricos o mediante la conservación de muestras de ADN, celulares o huellas dactilares, entre otros.

Todo ello, se considera dentro del concepto “vida privada” acuñado por la jurisprudencia y el Convenio 108, de manera que es posible proteger el tratamiento de los datos personales referentes a todos estos aspectos, mediante la tutela ofrecida por el derecho consagrado bajo el art.8 CEDH. Esto supone que el art. 8 CEDH es un derecho que ha rebasado muchas concepciones clásicas de lo que es la privacidad, con tal de ofrecer una protección eficaz a las personas. En este sentido, lo que muchos autores han denominado “derecho a la intimidad”, también entra dentro de la concepción de “vida privada” para el TEDH. A modo ilustrativo, parece oportuno reproducir la categorización de Arzoz Santisteban sobre los diferentes aspectos que componen el derecho al respeto de la vida

¹⁴¹ RUIZ ZAPATERO, G., “El TEDH y la protección de la privacidad de los datos tributarios”. *Revista Quincena Fiscal*, num.5, 2016 (parte Estudio, Editorial Aranzadi, S.A.U., Cizur Menor. 2016. p.1-6, p.6.)

¹⁴² PETTITTI, L.-E.: *La convention européenne des droits de l'Homme*, Economica, Paris, 1999, p. 305-32.

privada y familiar, domicilio y correspondencia, como son:

- “a) la integridad física y moral, interrupción del embarazo inclusive;
- b) el derecho a la propia apariencia externa, la propia imagen y la propia reputación;
- c) los derechos al nombre, al estatus familiar y al conocimiento del pasado;
- d) la vinculación y el arraigo en un territorio determinado como ámbito protegido;
- e) el derecho a ejercer una actividad profesional;
- f) la protección frente a las agresiones al medio ambiente que afectan a la calidad de la vida privada (ruidos, malos olores, emisiones);
- g) la vida y orientación sexual;
- h) la recopilación, conservación, utilización y revelación de datos personales o confidenciales;
- i) las técnicas y procedimientos de investigación policial;
- j) la libertad de movimiento;
- k) el modo de vida de las minorías étnicas, en particular de la comunidad gitana”¹⁴³.

Como ya se ha dicho, el hecho de que la protección de datos personales esté inserta en el art. 8 CEDH ha supuesto que la tutela ofrecida por el Tribunal a lo largo de su desarrollo, sea muy similar al tratamiento conferido al art. 8 CEDH antes de su reconocimiento. Por ello, los principios para analizar si ha habido una vulneración del art. 8 CEDH, y, por tanto, en la protección de datos personales, son, en gran medida, los mismos. Es decir, se vuelve a repetir el *principio de tratamiento lícito de los datos o de injerencia justificada*, con todos los aspectos que conlleva.

No obstante, a lo largo de su desarrollo en el s. XXI, han ido apareciendo principios adicionales, esta vez propios de la protección de datos. Así, *el principio de conservación de los datos*, que, si bien, no aparece en todos los casos, viene a significar que los Estados deben garantizar que los datos personales son conservados de manera que sea posible identificar a los individuos, por un tiempo no mayor al necesario para los fines que fueron recolectados, o con respecto a los fines para los que vayan a ser tratados posteriormente.

¹⁴³ ARZOZ SANTISTEBAN, X.: *Convenio Europeo de Derechos humanos. Comentario sistemático*, Thomson-Reuters-Civitas, 2015, p. 338 y ss.

En otras palabras, que el tiempo de conservación sea limitado y proporcional respecto del fin para el que los datos han sido recogidos¹⁴⁴.

Otro principio que se ha podido apreciar ha sido el *principio de tratamiento leal*, que se configura desde una doble perspectiva: por un lado, la transparencia; y por otro, el establecimiento de confianza. En cuanto a la transparencia, este principio consiste, básicamente, en que los individuos cuyos datos son tratados deben ser informados de ello, además de qué datos son usados, de qué manera y para qué fin. Puede establecerse cierta relación con el derecho individual que se analizará posteriormente, que es el de acceso a los datos. En cuanto al establecimiento de confianza, tiene cierta relación con la transparencia. Supone que los interesados deben poder ser documentados sin demora sobre el tratamiento de sus datos, y conocer así que su tratamiento es lícito y transparente, en lugar de secreto y posiblemente negativo¹⁴⁵.

5.2.2. Relación con otros derechos

A diferencia de la etapa anterior, es en la jurisprudencia del s. XXI donde el Tribunal parece tener que ponderar el derecho contemplado en el art. 8 CEDH y, por consiguiente, la protección de datos personales con otros derechos del CEDH y sus Protocolos, fundamentalmente con la libertad de expresión y el derecho a la propiedad.

El primer derecho puesto en relación es el derecho a la *libertad de expresión*, consagrado en el art. 10 CEDH. Este derecho garantiza “la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras”. No es tampoco un derecho absoluto, de manera que el mismo artículo prescribe la posible limitación en el ejercicio del derecho, siempre que “esté prevista por la ley, y constituya una medida necesaria en una sociedad democrática, para (...) la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales”, haciendo alusión, por tanto, a la protección del derecho al respeto de la vida privada y familiar, domicilio y correspondencia del art. 8 CEDH, y por tanto, la posible protección de datos personales.

¹⁴⁴ AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, CONSEJO DE EUROPA, “Manual de legislación europea en materia de la protección de datos”, Belgium, 2014, p. 80. Disponible en <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf>. Consultado el 15 de julio de 2017

¹⁴⁵ *Ibid*, p. 80-82

Estos derechos se limitan, o ceden uno a otro, en la medida necesaria para ser conciliados, como se verá a continuación.

Respecto de la parte del derecho que concierne a la *libertad de opinión y de comunicar informaciones o ideas*, las limitaciones ocurren normalmente en asuntos donde hay fines periodísticos o de expresión artística. Los casos más numerosos son los periodísticos. Los criterios que el Tribunal establece para la ponderación de derechos en estos casos, son el hecho de que el artículo publicado fuera de interés general, si la persona concernida era un personaje público, y si la fuente de información era fiable. Y en general, da importancia al hecho de que la información expresada sea o no de interés general en términos globales. De esta manera, la parte de la vida privada que se protege en estos casos es, por ejemplo, fotografías de la rutina cotidiana de personajes famosos en la prensa¹⁴⁶. Es decir, la protección ante el conocimiento masivo, mediante la divulgación o publicación, de una información que se refiere a la vida privada de una persona, y que *a priori*, no tiene por qué ser revelada sin su consentimiento.

El segundo aspecto relacionado con el art. 8, es la libertad de las artes y de las ciencias, que también se encuentra protegida por el art. 10. Se trataría, por ejemplo, del supuesto de la utilización de imágenes del rostro de personajes públicos unidos con dibujos caricaturescos¹⁴⁷. Las personas afectadas no están conformes con el uso que se hace de una parte referente a su imagen que, como se sabe, entra dentro del término “vida privada” y en la tutela ofrecida por el art. 8 CEDH.

Cierto es que, en cuanto a la libertad de las ciencias, no se ha encontrado jurisprudencia ponderando los derechos mencionados, pero es probable que en algún momento aparezca, ya que, por ejemplo, la obtención de muestras biométricas, perfiles de ADN o muestras celulares es algo usual en la jurisprudencia del Tribunal bajo la protección del art. 8 CEDH. Un ejemplo de protección de la vida privada en este ámbito podría darse en el uso de datos personales que fueron recopilados para una finalidad inicial, y que sean usados después con fines de investigación científica.

Dentro de este derecho, la *libertad de recibir información* también es importante. Sobre todo, en cuanto se refiere al acceso a los documentos gubernamentales o de autoridades

¹⁴⁶ TEDH, *Von Hannover v. Germany* (nº 2) [GC], (nº40660/08 and 60641/08), sentencia de 7 de febrero de 2012

¹⁴⁷ TEDH, *Vereinigung bildender Künstler v. Austria*, (nº68345/01), sentencia de 25 de enero de 2007

públicas, aspecto que se sabe necesario en las sociedades democráticas. Así, el Tribunal también ha conocido de casos en los que se ha ponderado el derecho a la vida privada y familiar con la libertad de expresión en este aspecto, defendiendo en pos del segundo, por ejemplo, el derecho que tienen los ciudadanos a conocer información de interés público o general. Así, un ejemplo de esta ponderación de derechos, se ha dado en un caso en que las autoridades denegaron el suministro de cierta información a una ONG, que quería obtenerla para realizar un fórum de debate público. Y esa información fue denegada precisamente por contener aspectos de la vida privada de un individuo que estaba envuelto en un pleito judicial¹⁴⁸. Así, esa información entra dentro del concepto “vida privada” y puede ser tutelada por el art. 8 CEDH. De esta manera, colisionan el derecho de los ciudadanos a conocer información de interés público mediante la iniciativa de la ONG, y el derecho al respeto a la vida privada respecto a los datos referentes al procesado, prevaleciendo en este caso, el primero, según el criterio del Tribunal atendiendo a las circunstancias del caso.

Otro derecho relacionado con el art. 8, pero en menor medida, es el derecho a la propiedad protegido por el Protocolo Adicional al CEDH nº. 1. Por ejemplo¹⁴⁹, en los casos de *copyright* de obras musicales, donde se ha alegado el interés público de la difusión y el acceso a las mismas¹⁵⁰. En este caso, en realidad, no se habla de una ponderación estricta de derechos entre la propiedad y la vida privada, pero sí se relacionan en cierta forma. Y es que, hay plataformas en Internet que ofrecen la posibilidad de descargar gratuitamente títulos musicales incluso si están protegidos por derechos de autor. Entonces, ambos derechos se relacionan, en la medida en que se pretende que el autor deba renunciar al poder de disposición de una obra propia de su creación, sobre la que él debería poder elegir a quién mostrar y bajo qué condiciones, en favor del interés general de que todo el público la conozca permitiendo su conocimiento y acceso ilimitado, y suponiendo además un tratamiento de la misma y su divulgación¹⁵¹.

Finalmente, cabe concluir que los casos donde el Tribunal realiza una ponderación expresa de derechos en los que uno de ellos sea la vida privada y familiar, son más bien

¹⁴⁸ TEDH, *Társaság a Szabadságjogokért v. Hungary*, (nº37374/05), sentencia de 14 de abril de 2009

¹⁴⁹ Cabe también destacar el caso TEDH, *Ashby Donald and others v. France*, (nº36769/08), sentencia de 10 de enero de 2013. RESEARCH DIVISION, "Internet: case-law of the European Court of Human Rights", Consejo de Europa, 2015, p. 39. Disponible en http://echr.coe.int/Documents/Research_report_internet_ENG.pdf. Consultado el 9 de septiembre de 2017.

¹⁵⁰ TEDH, *SIA AKKA/LAA v. Latvia*, (nº562/05), sentencia de 12 de julio de 2016

¹⁵¹ AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, CONSEJO DE EUROPA, “Manual de legislación europea en materia de la protección de datos”, Belgium, 2014, p. 36. Disponible en <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf>. Consultado el 15 de julio de 2017

pocos. Es decir, normalmente, el derecho al respeto de la vida privada y familiar no suele entrar en colisión con derechos de terceros. Más bien, en la mayoría de los casos, el TEDH suele ceñirse sólo a examinar si ha habido vulneración del derecho por parte del Estado. Así, cuando hablamos de la colisión del derecho a la protección de datos personales con otros derechos (siempre dentro del art. 8 CEDH), los casos examinados en este sentido son igualmente muy escasos, de manera que la protección de los datos personales también se caracteriza por no entrar en colisión con otros derechos, en la mayoría de los casos que llegan al Tribunal¹⁵². En este sentido, hay que entender que el Tribunal resuelve asuntos que se refieren a la vulneración del derecho por parte del Estado. Por lo tanto, los casos suelen ir mucho más dirigidos a dilucidar si ha habido una injerencia, y su adaptación o no al principio de licitud de la injerencia o injerencia justificada, mencionando pocas veces el conflicto de derechos (que suele producirse más entre particulares, y en estos casos, sólo se puede demandar al Estado si no ha regulado correctamente alguna obligación positiva para proteger un derecho).

Además, generalmente, cuando hablamos de protección de datos personales, esta protección se refiere básicamente al tratamiento de los mismos, es decir, ante operaciones como su almacenamiento, uso, conservación, divulgación... Luego no es lo más común que en estos casos se den colisiones de derechos de diferentes personas. Es más lógico que esta concurrencia de derechos sea más propia de otros de los numerosos ámbitos que componen el derecho al respeto de la vida privada y familiar, más que en el ámbito concreto del tratamiento de los datos personales.

5.2.3. Acciones de las personas

La recopilación de datos, su conservación, su uso o divulgación, es decir, el tratamiento de los datos personales, pueden constituir injerencias en el derecho a la vida privada y familiar. De esta manera, como queda consolidado en la jurisprudencia del s. XXI, los individuos deben estar facultados por la legislación nacional para proteger su vida privada ante estas injerencias, mediante diversos mecanismos y derechos. Pero a veces, por diversas circunstancias, tales como otros intereses protegibles por el Estado, derechos de otras personas, o porque la legislación interna no prevé mecanismos adecuados, los

¹⁵² TEDH, *Társaság a Szabadságjogokért v. Hungary*, (nº37374/05), sentencia de 14 de abril de 2009

interesados no pueden ejercer esos derechos. Por ello, acuden al TEDH como última instancia, que ponderará la situación estableciendo si ello constituye una injerencia al derecho a la vida privada y familiar, permitiendo o no el ejercicio de tales derechos o mecanismos de protección que han resultado denegados o imposibles de ejercer en el Estado concreto. De esta manera, con arreglo al derecho nacional, debe ser posible que los interesados tengan derecho básicamente a los siguientes aspectos: el acceso a la información personal, la rectificación o supresión de datos y la oposición al tratamiento de la información.

En cuanto al primer supuesto, es decir, el acceso a la información personal, aunque hay limitaciones legítimas para que las autoridades denieguen este derecho en un momento puntual, según las prescripciones del art. 8.2 CEDH; por regla general, el Tribunal establece en su jurisprudencia que es un derecho que debe reconocerse en aras a garantizar el ejercicio efectivo del derecho al respeto de la vida privada y familiar del art.8 CEDH, y en particular, para la protección de los datos personales. Así, existe un derecho de acceso a la información que consista en datos personales conservados o utilizados por otras personas. Este derecho supone que el individuo tiene la necesidad de conocer cierta información en poder de otros que le puede afectar de muy diversa forma. Por ejemplo, para conocer su capacidad reproductiva o estado de salud, para conocer su pasado o identidad, y en general, conocer toda la información que sea relevante y apropiada para la protección de su vida privada y familiar¹⁵³.

De ello, generalmente, se derivarán además sucesivos derechos. Por ejemplo, para poder rectificar u oponerse a una información incorrecta o falsa que concierne a su vida privada, a veces es necesario primeramente conocer qué información posee la autoridad pública o un tercero sobre uno mismo. Además, el Tribunal ha afirmado que el derecho de acceso a la información debe ser práctico y efectivo, haciendo posible, por ejemplo, hacer fotocopias de tal información cuando sea necesario.

Por lo que se refiere a la rectificación o supresión de datos¹⁵⁴, también puede apreciarse en la jurisprudencia del Tribunal, que existe un derecho a la rectificación o supresión de información que contenga datos personales que sean erróneos, inexactos o falsos. Así, las legislaciones nacionales deben prever este tipo de mecanismos de corrección ante

¹⁵³ TEDH, *Odièvre v. France* [GC], (nº42326/98), sentencia de 13 de febrero de 2003; TEDH, *K.H. and Others v. Slovakia*, (nº32881/04), sentencia de 28 de abril de 2009

¹⁵⁴ TEDH, *Rotaru v. Romania* [GC], (nº28341/95), sentencia de 4 de mayo de 2000

posibles incidencias que plantee el interesado.

De este modo, por ejemplo, el interesado puede pedir que se modifiquen datos erróneos en cuanto a su etnia, la modificación de información obtenida sin pruebas en registros policiales o de autoridades públicas, la supresión del calificativo de prostituta en un registro policial cuando la persona no ejercía dicha actividad, o la supresión de cierta información en un registro que llevaba demasiado tiempo conservada y ya no era necesaria para los fines para los cuales fue recopilada. La denegación por parte de la legislación nacional de estos derechos, entre otros casos, suponen una injerencia y vulneración del derecho al respeto de la vida privada y familiar por parte de los Estados.

Por último, en materia de oposición al tratamiento de la información, debido a una situación concreta del interesado¹⁵⁵; esta garantía es mucho menos común. Es difícil encontrar una legislación nacional que prevea esta garantía de acuerdo a la protección de la vida privada, ya que la problemática es casuística y escasa. En este sentido, el TEDH, ha establecido que no existe un derecho general de oposición al tratamiento de los datos personales. Normalmente, una oposición al tratamiento vendrá legitimada por una situación particular que una persona esté viviendo y suponga, a su juicio, una vulneración del respeto a su vida privada y familiar. Así, el Estado, y el TEDH en última instancia, deberá encontrar un equilibrio entre la protección del respeto a la vida privada y familiar del interesado, y los otros intereses o derechos en conflicto, ambos encontrados en el tratamiento de esa información personal¹⁵⁶.

Un ejemplo de ello podría ser la información recogida y almacenada en una clínica en relación con el tratamiento médico de un individuo, y su comunicación posterior a un tercero, sin el consentimiento del afectado y sin posibilidad de oposición. Otro ejemplo podría ser, el caso en el que el demandante se quejó de que las autoridades públicas no habían impuesto una obligación jurídica al responsable del tratamiento de sus datos de notificarlo por adelantado, a fin de permitirle la oportunidad de solicitar una medida cautelar e impedir así la publicación de material que violara su derecho al respeto de su vida privada¹⁵⁷.

¹⁵⁵ TEDH, *M.S. contra Suecia*, (nº20837/92), sentencia de 27 de agosto de 1997

¹⁵⁶ AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, CONSEJO DE EUROPA, “Manual de legislación europea en materia de la protección de datos”, Belgium, 2014, p. 124. Disponible en <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf>. Consultado el 15 de julio de 2017

¹⁵⁷ TEDH, *M.S. contra Suecia*, (nº20837/92), sentencia de 27 de agosto de 1997; TEDH, *Mosley contra el Reino Unido*, (nº48009/08), sentencia de 10 de mayo de 2011

5.2.4. Obligaciones de los Estados

Durante el s. XXI, las obligaciones negativas siguen existiendo de la misma manera en que lo hacían durante el s. XX. Los Estados siguen teniendo la responsabilidad de abstenerse de cometer injerencias en el derecho al respeto a la vida privada y familiar, y, por lo tanto, también en lo que respecta a la protección de los datos personales. En cuanto a las obligaciones positivas, se vio que el antecedente más importante se encontraba en el caso *Gaskin c. Reino Unido*. Esta jurisprudencia se consolida en el s. XXI. El Tribunal ha reiterado, además, que existen diferentes formas de garantizar el respeto de la vida privada, y que la naturaleza de la obligación del Estado dependerá del aspecto particular de la vida privada que está en cuestión. Así, la elección de los medios para asegurar el cumplimiento del artículo 8 está, en principio, dentro del margen de apreciación del Estado (aunque a veces el TEDH sí establece algunas obligaciones concretas).

De esta manera, la tipología de obligaciones positivas que debe cumplir el Estado para garantizar el respeto a la vida privada es variada. Puede ocurrir que el Estado tenga que intervenir incluso en las relaciones entre particulares, y, así, efectúe cambios en la legislación o en la jurisprudencia si fuera preciso. Algunos ejemplos constatados podrían ser que la legislación, a pesar de imponer diversas obligaciones de confidencialidad, deba ser modificada para que se permita a un menor identificar y enjuiciar al autor de una publicación en internet sobre anuncios con carácter sexual sobre su persona. También, es necesario que el Estado permita en términos generales el acceso a diferentes tipos de información, es decir, a toda aquella que en general sea relevante y apropiada para asegurar el respeto y el ejercicio de su derecho, así como hacer copias de esa misma información.

Asimismo, el Tribunal puede apreciar que el Estado demandado ha cumplido debidamente sus obligaciones positivas en el caso concreto, y así, se ha dado la no admisión de una demanda por estas razones. En esta misma línea, ha habido casos sí admitidos en los que Tribunal ha considerado que el Estado ha cumplido debidamente sus obligaciones positivas, para garantizar el ejercicio efectivo del derecho al respeto a la vida privada. Porque, los Estados, para cumplir con estas obligaciones, tienen un margen de apreciación para tomar las medidas correspondientes, y el Tribunal, puede decidir si tal margen de apreciación ha sido correcto o no en aras de la protección del derecho. Así, por ejemplo, el Tribunal ha considerado que el Estado en cuestión ha ponderado

debidamente los derechos en conflicto y ha cumplido con sus obligaciones positivas, permitiendo a un empresario proteger su derecho de propiedad y obtener una sentencia favorable habiendo grabado mediante video-vigilancia encubierta a su empleada en el acto de hurto en su tienda. En este caso, se había demandado al Estado por incumplimiento de una obligación positiva (haber permitido a ese empresario obtener una sentencia favorable usando aspectos de la vida privada de su empleada), pero el Tribunal, falló a favor del Estado por considerar cumplidas tales obligaciones.

Lo cierto es que, aunque las demandas al TEDH realmente van dirigidas únicamente contra los Estados Parte del CEDH como causantes de la violación del derecho, también pueden dirigirse indirectamente contra acciones u omisiones de personas privadas. Es decir, que las demandas que llegan al Tribunal, normalmente son verticales (Estado-individuo), pero cabe la posibilidad de que sean horizontales (relación individuo-individuo, por responsabilidad indirecta del Estado) dado que el Estado debe cumplir con sus obligaciones positivas con arreglo al CEDH, es decir, debe dotar de una protección suficiente contra los incumplimientos por parte de los particulares de los derechos de protección de los datos personales, contemplados en su Derecho nacional¹⁵⁸.

Durante el s. XXI, por tanto, el desarrollo de las obligaciones positivas de los Estados en lo que respecta a la garantía del art. 8 CEDH es mayor, pero en el ámbito concreto de la protección de datos, la mención expresa de esta área por el Tribunal es escasa¹⁵⁹. Se piensa que se debe, básicamente, a las mismas razones explicadas con anterioridad. Quizá, la novedad más destacada en relación con el ámbito de las obligaciones positivas en el área de la protección de datos es la mención al Convenio 108. Así, el TEDH se refiere a la equiparación práctica de la tutela del derecho a la vida privada y familiar que los Estados deben proporcionar para garantizar este derecho en relación con la protección de los datos personales, con diferentes preceptos del Convenio 108 que también tutelan este aspecto¹⁶⁰. Es decir, establece que la legislación interna debe ofrecer garantías apropiadas para la protección de los datos personales para así asegurar la tutela del art. 8 CEDH, derecho en el que se incardina. Y que tales garantías deben ser conformes a

¹⁵⁸ AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, CONSEJO DE EUROPA, “Manual de legislación europea en materia de la protección de datos”, Belgium, 2014, p. 134. Disponible en <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf>. Consultado el 1 de julio de 2017.

¹⁵⁹ TEDH, *K.H. y otros contra Eslovaquia*, (nº32881/04), sentencia de 6 de noviembre 2009

¹⁶⁰ TEDH, *Z. c. Finlandia*, (nº22009/93), sentencia de 25 de febrero de 1997; TEDH, *M.S. contra Suecia*, (nº20837/92), sentencia de 27 de agosto de 1997; TEDH, *Mosley contra el Reino Unido*, (nº48009/08), sentencia de 10 de mayo de 2011

diversos preceptos del Convenio 108. Entre otros, por ejemplo, los arts. 5 y 6, que se refieren a los principios en el tratamiento de los datos personales en general¹⁶¹, y de las garantías específicas que requieren ciertas categorías particulares de datos, los datos “más sensibles”. Así, el Tribunal transmite a los Estados que para garantizar el derecho al respeto a la vida privada del art. 8 CEDH, en lo que se refiere al área de protección de datos personales (como sabemos, área de protección autónoma dentro del art. 8 CEDH), se deben adoptar las medidas que dispone el Convenio 108 para garantizar satisfactoriamente su protección.

5.3. EVOLUCIÓN: LA INCIDENCIA DE LA TECNOLOGÍA DEL S. XXI EN LA JURISPRUDENCIA DEL TEDH

Como se ha podido observar en anteriores apartados de este trabajo, la protección de datos personales tiene una estrecha relación con el crecimiento del uso de las nuevas tecnologías en general. Tal es su importancia, que una de las razones por las que el Convenio 108 está siendo modernizado, es porque su crecimiento exponencial se concibe como un factor de riesgo para la protección de los datos personales. Así, la idea que subyace en este apartado, es analizar qué nuevas tecnologías son las que acompañan a los casos que llegan al Tribunal, a efectos de determinar nuevas posibles vulneraciones a la protección de datos personales. Esto permitirá saber si a estos efectos es apreciable la presencia de la tecnología y la ciencia más puntera en los casos que le llegan, y, por tanto, reflexionar sobre si esta vía es adecuada para la protección de este derecho frente a los nuevos retos tecnológicos¹⁶². Por orden de mayor a menor incidencia, la tecnológicas con más presencia en los casos que llegan al Tribunal, pueden categorizarse en las siguientes.

5.3.1. Internet, principal herramienta de interceptación de las comunicaciones

Esta es una de las áreas en las que las nuevas tecnologías tienen una mayor incidencia con respecto a la materia que nos ocupa, aunque también hay numerosos casos en los que

¹⁶¹ Ver capítulo 3, apartado 3.2.2. de este trabajo, referente a los principios en el tratamiento de los datos personales en el Convenio 108.

¹⁶² Para ver los casos correspondientes a este apartado, ver Anexo 10. La Jurisprudencia del TEDH en materia de protección de datos: casos con mayor incidencia de las nuevas tecnologías

se vulnera la libertad de expresión. Estas injerencias son, en general, perpetradas por las diferentes estructuras organizativas del Gobierno, y suele ser a organizaciones, más que a personas individuales.

Especialmente tiene relevancia la interceptación de las comunicaciones realizadas a través de Internet (incluyendo así al correo electrónico y datos de navegación almacenados en ordenadores de los individuos¹⁶³). Además, como la tecnología relacionada con la red ha avanzado mucho, actualmente tiene bastante relevancia los sistemas de vigilancia mediante la monitorización de comunicaciones *online*¹⁶⁴. Este aspecto es el que más presencia tiene en lo que se refiere a la interceptación de comunicaciones mediante las nuevas tecnologías, y el que de alguna manera es el más novedoso. Sin embargo, hay que destacar que muchos casos respecto a la interceptación de las comunicaciones vienen referidos a las tecnologías clásicas de la comunicación, como pueden ser la correspondencia, el teléfono o el facsímil.

La telefonía móvil y los proveedores de los servicios de telecomunicaciones también juegan un papel importante. Han llegado casos al Tribunal en los que se han producido la interceptación de comunicaciones de telefonía móvil, facilitada a la policía por parte de estos operadores, prácticamente sin restricciones. Asimismo, se han cuestionado las facultades de la policía para acceder directa e indistintamente a todos los datos de los proveedores de telecomunicaciones móviles. Y también, se ha puesto en duda la licitud de la obligación legal de los proveedores de telecomunicaciones de almacenar los datos personales de todos sus clientes.

En general, son pocos los casos en los que las nuevas tecnologías están presentes en la jurisprudencia, y algunos de ellos siguen pendientes. Por lo tanto, puede concluirse que,

¹⁶³ Private life includes the privacy of communications, which covers the security and privacy of mail, telephone, e-mail and other forms of communication; and informational privacy, including online information (*Copland v. the United Kingdom*, no. 62617/00, ECHR 2007-I). RESEARCH DIVISION, "Internet: case-law of the European Court of Human Rights", Consejo de Europa, 2015, p.8. Disponible en http://echr.coe.int/Documents/Research_report_internet_ENG.pdf. Consultado el 9 de septiembre de 2017

¹⁶⁴ For example, in the case of *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*, currently under examination, the applicants complain under Articles 8 and 10 of the Convention about the interception of communications, including on the Internet, (case no. 62322/14, communicated to the respondent Government on 5 January 2015).⁶ More precisely, they consider that the statutory regime in relation to the interception of external communications has affected their ability to undertake their work of investigative journalism without fear for the security of their communications. Ultimately, they argue, this poses a risk to the public watchdog role of the press. *Big Brother Watch and Others v. the United Kingdom* (no. 58170/13) is another case in point, which was communicated to the respondent Government on 7 January 2014.⁷ The applicants complain about the interception of communications by the intelligence services. This application, which is pending, concerns the compatibility with Article 8 of the collection, analysis, storage and destruction of the information thus intercepted. RESEARCH DIVISION, "Internet: case-law of the European Court of Human Rights", Consejo de Europa, 2015, p. 14, 15. Disponible en http://echr.coe.int/Documents/Research_report_internet_ENG.pdf. Consultado el 9 de septiembre de 2017

en el marco de la comunicación, aunque Internet aparece ya en algunos casos sustanciados ante el TEDH desde finales del s. XX, los casos más numerosos siguen haciendo referencia a métodos de comunicación clásicos, como pueden ser la correspondencia, telefonía, etc.; cuando actualmente el mundo de las comunicaciones tiene un espectro enormemente amplio.

5.3.2. Recogida de muestras de ADN relacionadas con la justicia penal

Esta área también es bastante significativa en cuanto al uso de las nuevas tecnologías. Prácticamente todos los casos que han llegado al TEDH bajo esta categoría se refieren al almacenamiento en una base de datos computarizada o informatizada, que suele ser nacional, de perfiles de ADN referentes a personas relacionadas con la justicia penal. Así, las demandas que llegan al Tribunal suelen referirse a la negación, por parte de los condenados a dar la muestra, ante una orden judicial de suministrarla. También han llegado casos en los que se solicita que las muestras tomadas sean eliminadas, de manera que no se permita su retención indefinida.

Pero el Tribunal, en estos casos, generalmente ha fallado que no hubo violación del art. 8 CEDH, y, por lo tanto, no ha considerado tales circunstancias suficientemente graves como para suponer una injerencia injustificada en la protección de datos personales. En este sentido, el Tribunal ha argumentado la existencia de un justo equilibrio encontrado por el Estado en cuestión, entre los intereses del particular y el interés público, para ordenar la recogida de tales muestras, particularmente de cara a la prevención del delito. También ha habido numerosos casos que se han declarado inadmisibles por diversas circunstancias (entre ellas, la de entender que este justo equilibrio está conseguido). Pero también ha habido casos en los que ha fallado en pro de la protección de estos datos personales. En estos casos, el Tribunal ha defendido que el uso de técnicas científicas modernas en el sistema de justicia penal no puede permitirse a cualquier costo, sin equilibrar cuidadosamente los beneficios potenciales del uso de tales técnicas contra intereses importantes de la vida privada. Así, ha establecido que cualquier Estado que reivindique la importancia del desarrollo de las nuevas tecnologías tiene la responsabilidad especial de lograr un equilibrio adecuado.

5.3.3. Técnicas de localización geográfica

La prevención frente a actos terroristas es otro de los elementos que el Tribunal defiende para permitir el uso de las nuevas tecnologías en la injerencia de los datos personales. En particular, ha defendido que proteger la seguridad nacional y los derechos de las víctimas son objetivos legítimos para permitir la obtención de información personal, por ejemplo, de tipo geográfica, suministrada por un dispositivo GPS colocado en un automóvil.

También ha establecido que, debido a las nuevas formas de terrorismo actual, es normal y natural que los gobiernos recurran a las tecnologías de vanguardia para evitar incidentes inminentes, protegiendo la seguridad nacional. Así, han llegado al Tribunal casos donde las medidas cuestionadas permitían incluso la posibilidad de vigilar masivamente las comunicaciones, interceptando masas de datos que podían incluir prácticamente a cualquier persona, incluso ajenas a las del objetivo original.

También se ha cuestionado la licitud de poder vigilar los movimientos geográficos de la vida privada de una persona, y almacenarlos en una base de datos de vigilancia. En este caso, el Tribunal indicó que el problema era la no regulación con suficiente claridad de las facultades discrecionales conferidas a las autoridades, para recopilar y almacenar esa información, y las garantías accesibles al público contra el abuso.

En resumen, el Tribunal, ante estas circunstancias, permite el uso de las nuevas tecnologías con estos fines. Pero estableciendo que es necesario que la legislación interna establezca las salvaguardias necesarias para evitar abusos, que las injerencias sean estrictamente necesarias, y que se puedan adoptar medidas correctivas efectivas.

5.3.4. Almacenamiento informático de datos personales y sus nuevos tratamientos: decisiones maquinizadas y acercamiento al Big Data

Hay alguna referencia en la jurisprudencia del TEDH a la incidencia de las bases de datos automatizadas sobre el derecho a la vida privada y familiar, y así, en la protección de datos personales. Por ejemplo, que, debido a una condena por un delito de violación de menores, un ordenador clasifique automáticamente al autor del delito en la base de datos

judicial referente a delincuentes sexuales. En este caso, lo importante es destacar la importancia de las bases de datos automatizadas que se pueden configurar de tal modo que puedan tomar decisiones que afecten a la protección de los datos personales.

El último caso a destacar se refiere a la publicación por dos compañías, de información fiscal de tipo personal de 1,2 millones de personas. Esta publicación masiva, según el derecho interno, había sido contraria a las leyes de protección de datos personales. Pero estas compañías acudieron al TEDH en busca de la defensa de su derecho a la libertad de expresión. En este caso, el Tribunal declaró la no violación de su derecho a la libertad de expresión y la prevalencia del objetivo de proteger la intimidad de los individuos. Pero con independencia del fallo, lo destacable en este caso es la tecnología que permite almacenar tal cantidad de información personal en manos de compañías privadas, lo que en cierta medida recuerda, aunque levemente, al Big Data; el reto a la privacidad más importante en los tiempos actuales.

VI. CONSIDERACIONES FINALES

1. Partiendo del análisis jurisprudencial como objeto troncal de la investigación, para obtener una conclusión fundada y contextualizada, ha sido necesario remontarse al origen de la protección de datos y entender su evolución y problemática actual; de manera que se pueda obtener un resultado integrado, teniendo en cuenta todos los factores que han podido influir y que influyen actualmente en la materia que nos ocupa. El estudio de este contexto nos ha llevado a la formulación de una primera consideración, que revisa el presupuesto inicial del que partíamos.

Así, debido al momento histórico actual y a la cantidad de información que cualquier individuo debe suministrar (y suministra sin querer) en su vida cotidiana, al comenzar esta investigación, se esperaba una protección mucho más eficaz y desarrollada, fruto de una conciencia asentada del problema y de los riesgos que entraña el poder de la información en el mundo contemporáneo. Por el contrario, la protección de datos personales, a pesar de ser una materia de nacimiento relativamente temprano (si tenemos como referencia la obra de *The Right to Privacy*, por *Warren y Brandeis*, publicada en 1890), es también una materia de discusión controvertida, que se caracteriza por una gran divergencia de razonamientos y de opiniones en cuanto a la definición y contenido del concepto. Y fruto de esta disparidad, se aportan soluciones realmente diferentes, incluso dentro de la protección que ha ofrecido el Consejo de Europa a lo largo de los años. Por lo tanto, en una primera aproximación a la materia, este desajuste actual a nivel local y global, resultó sorprendente y contrario a la hipótesis de una temática madurada por la doctrina y la sociedad.

2. La segunda consideración atiende al primer objetivo de la investigación: la actitud del TEDH respecto a la protección de los datos personales. Se pensaba que su jurisprudencia era el resultado de un *proceso* de estudio lineal y de *resultado* efectivo. Sin embargo, lejos de poder adentrarse en un análisis directo, centrado y acotado sobre la materia, la única forma de realizarlo ha resultado ser el análisis de un largo proceso de formación conceptual. Ofreciendo, además, como resultado, una actitud caracterizada por ser más esquiva e imprecisa, que directa y eficaz.

Desarrollando estos resultados, en lo que atañe al *proceso* de formación del concepto, éste ha sido de nacimiento extraordinariamente tardío en la jurisprudencia del Tribunal, cuya formación ha ido de la mano de la evolución tecnológica. Así, se confirma la hipótesis de la influencia directa de la tecnología en la existencia de la protección de datos personales mediante numerosos elementos. Por ejemplo, el número de casos que han llegado al Tribunal según se producía el avance tecnológico de la sociedad, las áreas concretas de vulneración del art. 8 CEDH totalmente vinculadas a la tecnología, etc. Pero, sobre todo, debido a que desde el mismo momento en el que el Tribunal reconoce la existencia de esta área de protección, su jurisprudencia remite al Convenio 108 como instrumento de referencia para que los Estados afronten satisfactoriamente la protección de los datos personales. En este tratado, se pone el énfasis en el tratamiento “automatizado” de los datos de carácter personal, de manera, que simplemente esta terminología ya revela que se protegen una serie de datos que están en íntima relación con la tecnología y la informática. En concreto, el Convenio 108 es mencionado para concretar la definición de “vida privada”, y, por ende, de protección de datos de carácter personal; pero también para equiparar la tutela que deben ofrecer los Estados en aras de la protección de los datos personales con las prescripciones del Convenio en la materia.

Esta presencia del Convenio 108 en la jurisprudencia del TEDH de manera simultánea al reconocimiento de la protección de los datos personales como elemento autónomo en el marco del art. 8 CEDH, refutó sin embargo otra hipótesis de la que partíamos inicialmente. Esta hipótesis consistía en que se pensaba que el Convenio 108 había sido elaborado de manera posterior al reconocimiento jurisprudencial del TEDH de la materia que nos ocupa. Así, se razonaba que el Convenio 108 había sido elaborado haciendo uso de la experiencia ofrecida por el TEDH, en cuanto a conocer las áreas más vulnerables y necesitadas de protección, y poder atajarlas de manera efectiva mediante la elaboración de un tratado internacional. Pero el resultado ha parecido ser el opuesto. Mientras que el Convenio 108 data de 1981, el primer caso jurisprudencial donde se reconoce expresamente la protección de datos es de 1997. De esta manera, resulta difícil entender que ha sido la jurisprudencia el motor de la redacción del Convenio 108, y, por lo tanto, puede concluirse que, más bien, se presenta éste como el factor que ha ayudado a la jurisprudencia del TEDH a reconocer la protección de los datos personales como un área necesitada de atención.

En lo que atañe al *resultado*, es decir, a la actitud o concepción final del Tribunal sobre el asunto, como se ha explicado anteriormente, se ha comprobado que éste ha alargado lo máximo posible el no reconocimiento. Y cuando finalmente lo ha hecho, no ha reconocido la protección de datos personales como un derecho humano fundamental con entidad propia, sino que lo ha concebido como una parte del derecho a la vida privada y familiar, domicilio y correspondencia, consagrado en el art. 8 CEDH; entendiendo que la protección de los datos personales es necesaria para garantizar el respeto a la “vida privada”, término que protege un bien jurídico extraordinariamente amplio.

Así, su concepción ha resultado ser más próxima a la “privacy” de Estados Unidos, explicada en la introducción de este trabajo, pero de manera incluso aún más amplia que ese concepto. Su actitud se ha erigido indiscutiblemente de manera contraria al resto de concepciones mayoritarias sobre la materia en el resto de Europa. Nada tiene que ver, por lo tanto, con la concepción imperante en el continente Europeo en general, ya que como se explicó, la Unión Europea percibe a la protección de datos personales como un derecho reconocido de manera autónoma, totalmente diferenciado del derecho a la vida privada y familiar; y difiere también de la doctrina mayoritaria de los países europeos que, como se ha visto, defienden el derecho a la autodeterminación informativa, libertad informática, u otros *nomen iuris* que hacen referencia a la autonomía del derecho. Aunque esta concepción extensiva del derecho del art. 8 CEDH es en parte comprensible. Es normal que en 1950 (fecha de adopción de la Convención Europea de Derechos Humanos) no se pudiera prever la evolución de la tecnología y su incidencia en ese derecho, de manera que llevara a un área de tan gran calado como lo es la protección de datos personales hoy en día. Además, el TEDH está muy limitado en su protección al CEDH, de manera que, si no se adoptara un Protocolo Adicional al mismo, proclamando el derecho a la protección de datos personales, no podría defenderlo de manera más directa. Pero el Consejo de Europa no optó por esta posibilidad, sino que ha decidido protegerlo mediante la adopción del Convenio 108, que, además, tampoco concibe la materia de una manera autónoma, sino también como parte integrante del derecho al respeto a la vida privada y familiar. Como su art.1 indica, este tratado protege “el derecho a la vida privada, con respecto al tratamiento de los datos automatizados de carácter personal”. Concibe así la protección de los datos personales de manera idéntica al Tribunal. Parece apreciarse, por tanto, en el CdE una reticencia generalizada a reconocer la autonomía al derecho a la protección de datos personales.

3. La tercera consideración está relacionada con la segunda. No cabe duda de que la influencia tecnológica es un hecho que ha contribuido de manera directa a la aparición de la protección de los datos personales en la jurisprudencia del Tribunal, como ha podido observarse a lo largo de toda la investigación. Pero, la expresión máxima de esta relación directa entre la protección de datos personales y la tecnología se encuentra en la actualidad debido al crecimiento exponencial que está experimentando. Sin embargo, en la jurisprudencia del TEDH, aunque esta presencia existe, es muy reciente y no muy abundante ni cuantitativamente, ni cualitativamente. Es decir, si hacemos una comparación con la tecnología que afronta la modernización del Convenio 108 (que, puede entenderse como la tecnología propia del s. XXI más actual y con incidencia en la protección de datos personales), no encontramos un reflejo total de ésta en los casos que llegan al Tribunal, a diferencia de lo que ocurría en los años propios del s. XX, en que esta traslación parecía bastante más cierta.

Así, pueden apreciarse en la jurisprudencia del Tribunal algunos factores tecnológicos que también aborda el nuevo borrador. Por ejemplo, la inclusión de los datos biométricos o perfiles de ADN en las categorías especiales de datos personales, con una protección reforzada. O también, el derecho a saber por qué un ordenador tomó una decisión automáticamente¹⁶⁵. Pero también hay muchos aspectos importantes en el nuevo borrador que no se vislumbran en la jurisprudencia, cuando en teoría, deberían estar por su supuesta gran incidencia en la protección de los datos personales, según el proyecto. Nos referimos fundamentalmente a los nuevos retos a la privacidad que plantea el Big Data. El único caso parecido es la publicación de las compañías de los datos fiscales de 1,2 millones de personas, pero faltan características que nos hagan entender que realmente estamos ante un supuesto en que el Big Data es el causante de la injerencia. Tampoco se encuentra referencia a los datos anónimos, ni a la tan destacada transferencia internacional de datos, que no sólo se hace referencia a ella en la modernización del Convenio, sino también en el Convenio 108 y en su Protocolo. El reflejo de las más modernas tecnologías en la jurisprudencia del TEDH del s. XXI es, por tanto, parcial.

¹⁶⁵ TEDH, *S. and Marper v. United Kingdom*, (nº30562/04 y 30566/04), sentencia de 4 de diciembre de 2008.
TEDH, *B.B. v. Francia, Gardel v. France and M.B. v. France*, (nº5335/06), sentencia de 17 de diciembre de 2009

Todo esto provoca una curiosa reflexión. Y es que, teniendo en cuenta la relación que ha existido a lo largo de la historia entre la tecnología y la protección de los datos personales, así como su reflejo en la jurisprudencia del TEDH a lo largo de los años, resulta un poco chocante la situación actual. Siendo hoy el momento histórico álgido del desarrollo tecnológico en todos sus sentidos, no existe ese reflejo tan directo de la tecnología puntera en la protección de los datos personales que hace el Tribunal. Es cierto que llegan muchos casos cuantitativamente en los que se alega como vulnerado el art. 8 CEDH, relacionados con la tecnología en general, pero es la propia de la sociedad de la información (teléfono, cámaras fotográficas, etc.) más que la de la era digital en la que vivimos. Y no aparecen los elementos actuales (básicamente Big Data y transferencias internacionales de datos) que realmente suponen un peligro importante para la protección de los datos personales. De manera contraria a lo que se esperaba, la tecnología propia de la era digital está contribuyendo poco al avance de la protección de los datos personales por parte del TEDH.

De este modo, no puede decirse que exista una construcción jurisprudencial cierta, precisa y efectiva ante las mayores amenazas que hoy enfrenta la protección de los datos personales. Más bien, puede apreciarse que la protección está bastante limitada por el propio CEDH, y por la concepción que los Estados tienen sobre la materia. Habrá que estar al desarrollo jurisprudencial en la próxima década, para ver si esta reflexión se mantiene o, si por el contrario, llegan más casos relacionados con el Big Data y con los flujos transfronterizos de información personal.

4. La razón de por qué esto ocurre, según los resultados obtenidos, parece ser la siguiente. Estos nuevos retos a la privacidad (Big Data y transferencias internacionales de datos) tienen un gran valor económico, y provienen, prácticamente en su totalidad, del sector privado. Los Estados se muestran permisivos en su regulación. Incluso, el propio Convenio 108, que se erige como un gran hito en la protección de los datos personales, en realidad liberaliza las corrientes de estos datos entre los Estados Parte del Convenio, pero lo hace de una manera disimulada, bajo la proclamación de la “libertad de información sin consideración de fronteras”. En otras palabras, el Derecho nacional e internacional (al menos en lo que respecta al Convenio 108), regulan la protección de los datos personales haciéndose eco de la economía de mercado en la que vivimos, entendiendo que el poder de la información es una herramienta poderosa de la que no se

puede prescindir en términos económicos. Por ello, la capacidad de obtener información privada para estos fines se regula de manera permisiva y carente de garantías para el individuo, pues parece ser que en esta ponderación entre el gran interés económico que supone la información y la privacidad del individuo, gana el interés económico, tanto a nivel nacional como internacional. Pero esto no puede hacerse de manera evidente hacia el ciudadano. Por ello, se utilizan eufemismos como el del Convenio 108, utilizando “la libertad de información sin fronteras” en lugar de “los intereses económicos sin fronteras”.

Ni los Estados ni el CdE parecen ser conscientes del alcance que puede llegar a tener esta protección. Y si lo son, no se aprecia una acción suficiente en respuesta. Este hecho se ve en parte agravado y en parte enmendado por lo siguiente. Agravado, porque, como se sabe, el TEDH protege los derechos humanos consagrados en el CEDH respecto de las injerencias injustificadas que puedan perpetrar los Estados. De esta manera, si los datos personales se ven desprotegidos por el tratamiento, normalmente lucrativo, que una empresa pueda hacer, es difícil demandar al Estado por tal situación. En primer lugar, porque, como se ha visto, la única manera de poder trasladar la responsabilidad al Estado es básicamente mediante el incumplimiento de alguna obligación positiva en garantía del art. 8 CEDH. Además, el CEDH permite ciertas injerencias en el disfrute del derecho a la protección de datos personales, siempre que estén previstas por la ley y mientras persigan fines legítimos, entre los cuales, el art. 8.2 proclama “el bienestar económico del país”. Es decir, los Estados tienen un margen de apreciación respaldado por el Derecho (art.8.2 CEDH) para hacer una ponderación de intereses a la hora de garantizar el derecho al respeto de la vida privada, de manera que pueda haber una injerencia en los datos personales del individuo que sea lícita y no suponga la vulneración del derecho si hay un fin legítimo que lo permita, y entre estos fines, se encuentra el fin lucrativo apuntado.

Pero este planteamiento también se ve en parte enmendado en el marco del Convenio 108. El CdE parece ser consciente de esta problemática y en un intento por aportar alguna solución ha optado por hacer un llamamiento a los Estados a que, en cierta manera, otorguen al individuo ciertas garantías mínimas ante los posibles abusos que se puedan hacer mediante el tratamiento de sus datos, en este *status quo* de carácter económico de la información.

5. En definitiva, en todo este proceso de investigación se ha podido comprobar una falta de protección adecuada de los datos personales tanto a nivel global como regional, que atiende, por una parte, a la difícil lucha contra el interés económico que impera en la actualidad, y por otra parte, a la imprecisión del desarrollo en el futuro, que plantea que el desafío de proteger los datos personales ante la velocidad del desarrollo tecnológico, hace parecer que los esfuerzos de protección paralelos sean en vano¹⁶⁶.

A nuestro juicio, el valor económico de la información y las posibilidades que la tecnología puede ofrecer a este fin, suponen hoy el principal problema para el respeto de la dignidad del individuo. Parece que la sociedad no es consciente de que, por aceptar las comodidades innegables que la tecnología nos ofrece hoy en día, estamos vendiendo el respeto a los aspectos más íntimos de nuestra personalidad a cualquier o ningún precio. Como dice THORBJØRN, “el advenimiento de las nuevas tecnologías de la comunicación está cambiando el mundo como la hilandería transformó la industria textil y las economías del mundo, y como nadie podía prever el impacto a largo plazo de la Revolución industrial”¹⁶⁷. Sin caer en visiones apocalípticas, es necesario ser conscientes de este fenómeno, y reflexionar para la búsqueda de soluciones efectivas.

¹⁶⁶ POLAKIEWICZ, J. *op. cit.*, p. 8 y 9

¹⁶⁷ THORBJØRN JAGLAND, “A new era for privacy”, 2011. Disponible en <http://www.coe.int/en/web/data-protection/articles-speeches-and-presentations>. Consultado el 10 de julio de 2017.

BIBLIOGRAFÍA

1. Artículos y monografías

- AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, CONSEJO DE EUROPA, “*Manual de legislación europea en materia de la protección de datos*”, Belgium, 2014. Disponible en fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf. Consultado el 1 de mayo de 2017
- ARZOZ SANTISTEBAN, X., “Derecho al respeto de la vida privada y familiar” en ARZOZ SANTISTEBAN, X., *Convenio Europeo de Derechos Humanos: Comentario sistemático*, Estudios y Comentarios Legislativos (Civitas). Editorial Aranzadi, S.A.U., enero de 2009
- ARZOZ SANTISTEBAN, X., “Recopilación, conservación, utilización y revelación de datos personales o confidenciales” en ARZOZ SANTISTEBAN, X., *Convenio Europeo de Derechos Humanos: Comentario sistemático*, Estudios y Comentarios Legislativos (Civitas). Editorial Aranzadi, S.A.U., enero de 2009
- BARCELONA LLOP, J., “Escuchas telefónicas y acción de policía de seguridad (A partir de la sentencia del TEDH sobre el caso <<Malone>>)”. *Revista de Administración Pública*. Núm. 112, enero-abril 1987, pp. 61-105
- DE MIGUEL ASENSIO, P. A., “Protección de datos personales”, en DE MIGUEL ASENSIO, P. A., *Derecho Privado de Internet*, Estudios y Comentarios Legislativos (Civitas). Editorial Aranzadi, S.A.U., Enero de 2015.
- DE SALAS MURILLO, S., “Sobre el alcance del ámbito de la protección de la vida privada y familiar en la jurisprudencia de Estrasburgo”, *Rev. Boliv. de Derecho*, No 23, enero 2017, pp. 194-207
- DIEZ DE VELASCO VALLEJO, M., “Capítulo XXVIII. La protección internacional de los derechos humanos (II)”, en DIEZ DE VELASCO VALLEJO, M., *Instituciones de Derecho Internacional Público*, 18ª Edición, Tecnos, Madrid, 2013
- ESTADELLA YUSTE, O., *La protección de la intimidad frente a la transmisión internacional de datos personales*. Madrid: Tecnos. 1995.
- GARCÍA-CUEVAS ROQUE, E. “Las transferencias internacionales de datos y las libertades individuales: un acercamiento a las normas de protección de datos*”, *Estudios de Deusto*, Vol. 60/2, Bilbao, Julio-Diciembre 2012, pp.171-194
- GARRIAGA DOMINGUEZ, A., *Nuevos retos para la protección de datos personales en la era del big data y de la computación ubicua*, Dykison, 2016.

- GARZÓN CLARIANA, G. "La protección de los datos personales y la función normativa del Consejo de Europa", *Revista de Instituciones Europeas*, Vol 8. Nº.1, (Enero-Abril 1981), pp.9-25
- GERALDES DA CUNHA LOPES, T.M, "El Derecho a la Intimidad y la Protección de Datos en la era de la Seguridad global. Principios constitucionales versus riesgos tecnológicos", *Anuario Jurídico y Económico Escurialense*, XLVIII (2015), p. 159-180
- GONZÁLEZ FUSTER, G., "TEDH – sentencia de 04.12.2008, s. y Marper c. Reino Unido, 30562/04 y 30566/04 – artículo 8 CEDH – vida privada – injerencia en una sociedad democrática – los límites del tratamiento de datos biométricos de personas no condenadas." *Revista de Derecho Comunitario Europeo*, núm. 33, Madrid, mayo/agosto (2009), págs. 619-633
- GRACIA BLANCO, M., "Mirando por detrás de la protección de datos: un paseo por la ley orgánica de tratamiento automatizado de datos de carácter personal, el "Data Protection Act" y la convención 108", *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, Nº 3, 1997, págs. 1916-1917
- GREENLEAF, G. "Balancing globalisation's benefits and commitments: accession to data protection convention 108 by countries outside Europe", *The global context of Convention 108 'globalisation'*, Conference Presentation, 2016
- GREENLEAF, G. " 'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?", *Computer Law & Security Review*, Vol 29, Issue 4, forthcoming, July/August 2013, pp.1-11
- GREENLEAF, G. "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?", *Edinburgh School of Law Research Paper Series*, No 2012/12, 2012
- GUASCH PORTAS, V., *Las transferencias internacionales de datos en la normativa española y comunitaria*, Tesis doctoral, Madrid, 2013
- GUDÍN RODRIGUEZ-MAGARIÑOS, F., "Requiem por el derecho a la intimidad en los smartphone: análisis de la última Jurisprudencia del TC contrastada con la del TEDH". *Revista Aranzadi Doctrinal*, num.9/2014, 2014, pp.1-15
- GUTIÉRREZ CASTILLO, V.L., "Aproximación a la protección jurídica internacional del derecho de acceso y protección de datos en Europa", *Derecho y conocimiento*, volumen 3, pp.1-19
- KUNER, C., "An international legal framework for data protection: Issues and prospects", *Computer Law & Security Review*, Volume 25, Issue 4, July 2009, Pages 307-317
- MARTÍNEZ MARTINEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Colección "Protección de datos", THOMSON CIVITAS, 2004

- MURILLO DE LA CUEVA, P.L., “El derecho a la autodeterminación informativa y la protección de datos personales”, *Azpilcueta*, N°. 20, 2008, pp.53-58
- MURILLO DE LA CUEVA, P.L., *El derecho a la autodeterminación informativa: La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*, Fundación Coloquio Jurídico Europeo, Madrid, 2009
- M. SCHWARTZ, P., “European Data Protection Law and Restrictions on International Data Flows”, 80 *Iowa L. Rev.*, 1994-95, pp. 471-496
- ORTEGA JIMÉNEZ, A., *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, Tesis doctoral, Alicante, 5 de septiembre de 2014
- ORTI VALLEJO. A., “El nuevo derecho fundamental (y de la personalidad) a la libertad informática”, *Derecho Privado y Constitución*, Núm. 2, enero-abril 1994, pp.305-332
- PÉREZ LUÑO, A.E., “Estado constitucional y derechos de la tercera generación”. Universidad de Sevilla. *Anuario de filosofía del Derecho* XIV (1997), pp.545-570
- PÉREZ LUÑO, A.E., “La tutela de la libertad informática en la sociedad globalizada”, *ISEGORIA* 22 (2000)
- PÉREZ LUÑO, A.E., “Las Generaciones de Derechos Humanos”, *Revista del Centro de Estudios Constitucionales* 203, Núm. 10. Septiembre-Diciembre 1991, pp.203-2117
- PETTITTI, L.-E.: *La Convention Européenne des droits de l’Homme*, Económica, Paris, 1999
- PIÑAR MAÑAS, J.L., *El Derecho a la autodeterminación informativa: Protección de datos: origen, situación actual y retos de futuro*, Fundación Coloquio Jurídico Europeo, Madrid, 2009
- POLAKIEWICZ, J. “International Data Protection Conference Convention 108 as a global privacy standard?”, Protection conference in Budapest, 17 June 2011. Disponible en <http://www.coe.int/en/web/data-protection/reports-studies-and-opinions>. Consultado el 25 mayo de 2017
- PAVÓN PÉREZ, J.A., "La Protección de Datos Personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales", *Anuario de la Facultad de Derecho*, N° 19-20, 2001-2002, pp.237-252
- RESEARCH DIVISION, "Internet: case-law of the European Court of Human Rights", Consejo de Europa, 2015. Disponible en http://echr.coe.int/Documents/Research_report_internet_ENG.pdf. Consultado el 9 de septiembre de 2017

- ROUVROY, A., "Of data and men" Fundamental rights and freedoms in a world of big data", Council of Europe, T-PD-BUR(2015)09REV. Disponible en [http://www.coe.int/en/web/data-protection/reports-studies-and-opinions#{"20422099": \[2\]}](http://www.coe.int/en/web/data-protection/reports-studies-and-opinions#{). Consultado el 25 de mayo de 2017
- RUIZ MIGUEL, C., "El Derecho a la Protección de los Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea: Análisis Crítico", *Revista de Derecho Comunitario Europeo*, Núm. 14, (enero-abril 2003), pp. 7-43
- RUIZ ZAPATERO, G., "El TEDH y la protección de la privacidad de los datos tributarios". *Revista Quincena Fiscal*, num.5, 2016, p.1-6
- SALTOR, C.E., *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina*, Tesis doctoral, Madrid, 2013
- SÁNCHEZ GONZÁLEZ, M.A., *Implicaciones institucionales de la ley de protección de datos*, Tesis doctoral, Málaga, 2015
- SANTOLAYA MACHETTI, P., *La Europa de los Derechos: El Convenio Europeo de Derechos Humanos*, Centro de Estudios Políticos y Constitucionales, Madrid, 2005
- SERRANO MAÍLLO, I., "Derecho a la libertad de expresión en la jurisprudencia del Tribunal Europeo de Derechos Humanos: dos casos españoles" UNED. *Teoría y Realidad Constitucional*, núm. 28, 2001, pp. 579-596.
- SOLANGE MANQUEO RAMÍREZ, M., MORENO GONZÁLEZ, J., RECIO GAYO, M., "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario" *Rev. derecho (Valdivia)* vol.30 no.1 (versión on-line)
- SUÁREZ RUBIO, S. M., "Tribunal Europeo de Derechos Humanos y el derecho a la vida privada: los perfiles de la creación de un amplio derecho de privacidad." *Parlamento y Constitución*. Anuario, Nº 14, 2011, págs. 121-142
- THORBJØRN JAGLAND, "A new era for privacy", 2011. Consejo de Europa. Disponible en http://www.coe.int/en/web/secretary-general/opinion-articles-2011/-/asset_publisher/WLDThjITozj2/content/a-new-era-for-privacy-by-thorbj-rn-jagland?inheritRedirect=false&redirect=http%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fsecretary-general%2Fopinion-articles-2011%3Fp_p_id%3D101_INSTANCE_WLDThjITozj2%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1. Consultado el 17 de julio de 2017.
- WALTER, J.-PH., Chair of the T-PD Deputy Commissioner, Federal Data Protection and Information Commissioner, Switzerland, "The role of Convention 108 in the international cooperation", 2014. Disponible en <http://www.coe.int/en/web/data->

protection/reports-studies-and-opinions#{"20422099":[]}. Consultado el 25 de mayo de 2017

2. Documentación:

Tratados:

- CONSEJO DE EUROPA, *Convenio Europeo de Derechos Humanos*, CETS n° 005, de 4 de noviembre de 1950
- CONSEJO DE EUROPA, *Convenio 108 sobre el Tratamiento automatizado de datos de carácter personal*, CETS n° 108, de 28 de enero de 1981
- CONSEJO DE EUROPA, *Protocolo Adicional al Convenio 108, sobre Autoridades de Protección y Flujo Transfronterizo de Datos*, CETS n° 181, de 8 de noviembre de 2001

Resoluciones y recomendaciones:

- CONSEJO DE EUROPA, Comité de Ministros, Recommendation (89)14 sur les incidences éthiques de l'infection VIH dans le cadre sanitaire et social, Doc. CM/Rec(89)14, de 24 de octubre de 1989
- CONSEJO DE EUROPA, Asamblea Parlamentaria, Recommendation 509 (1968) on human rights and modern scientific and technological developments, de 31 de enero de 1968
- CONSEJO DE EUROPA, Comité de Ministros, Resolution (1973)22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector, CM/Res(1973), de 26 de septiembre de 1973
- CONSEJO DE EUROPA, Comité de Ministros, Resolution (1974)29, on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector, CM/Res(1974), de 20 de septiembre de 1974

Otros documentos:

- Borrador de la Modernización del Convenio 108 sobre el tratamiento automatizado de datos de carácter personal
- COUNCIL OF EUROPE, T-PD (2017)01, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasbourg, 2017. Disponible en <https://rm.coe.int/16806ebe7a>. Consultado el 1 de mayo de 2017
- Memoria explicativa del Borrador de la Modernización del Convenio 108 sobre el Tratamiento automatizado de datos de carácter personal

- Memoria explicativa del Convenio 108 sobre el Tratamiento automatizado de datos de carácter personal
- Memoria explicativa del Protocolo Adicional al Convenio 108, sobre Autoridades de Protección y Flujo Transfronterizo de Datos
- Secretariat of the Convention's Consultative Committee Directorate General of Human Rights and Rule of Law, "Accession to Convention 108 and to its additional Protocol by non-European States", 2011.
- TEDH: *Personal Data*, Factsheet, julio 2017. Disponible en http://www.echr.coe.int/Documents/FS_Data_ENG.pdf. Consultado el 20 de julio de 2017
- TEDH: *Mass Surveillance*, Factsheet, junio 2017. Disponible en http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf. Consultado el 20 de julio de 2017
- TEDH: *New Technologies*, Factsheet, julio 2017. Disponible en http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf. Consultado el 20 de julio de 2017
- Treaty Office del Consejo de Europa, "Chart of signatures and ratifications of Treaty 108" (Status as of 01/07/2017). Disponible en <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>. Consultado el 1 de julio de 2017.

3. Recursos web:

- Página oficial Tribunal Europeo de Derechos Humanos. Disponible en <http://www.echr.coe.int/Pages/home.aspx?p=home&c>. Consultado el 1 de julio de 2017
- Página oficial del Consejo de Europa. Disponible en <http://www.coe.int/en/web/portal/home>. Consultado el 1 de julio de 2017
- Página oficial de la UNED. Disponible en <http://ocw.uned.ac.cr/eduCommons/s.e.p/tecnologia-y-trabajo/tutorias/tutoria-segunda/autodeterminacion-informativa-y-estado-de-derecho-en-la-sociedad-tecnologica-alfredo-chirino/view>. Consultado el 1 de mayo de 2017

Anexo 1. La Jurisprudencia del TEDH en materia de protección de datos: datos generales			
CASO	FECHA	TEMÁTICA	DERECHOS EN CUESTIÓN
FACTSHEET: PERSONAL DATA			
Uzun v. Germany Ben Faiza v. France PENDING L.H. v. Latvia Klass and Others v. Germany Malone v. the United Kingdom Kruslin v. France Kopp v. Switzerland Amann v. Switzerland Taylor-Sabori v. the United Kingdom Visse v. France Kennedy v. the United Kingdom Dragojević v. Croatia R.E. v. the United Kingdom (no. 62498/11) Roman Zakharov v. Russia Szabó and Vissy v. Hungary Centrum För Rättvisa v. Sweden PENDING Tretter and Others v. Austria PENDING Big Brother Watch and Others v. the United Kingdom PENDING Bureau of Investigative Journalism and Alice Ross v. the United Kingdom PENDING 10 Human Rights Organisations and Others v. the United Kingdom PENDING Bîrbulescu v. Romania PENDING Libert v. France PENDING P.G. and J.H. v. the United Kingdom Vetter v. France Peck v. the United Kingdom Köpke v. Germany Antović and Mirković v. Montenegro PENDING Perry v. the United Kingdom S. and Marper v. the United Kingdom B.B. v. France, Gardel v. France and M.B. v. France Dimitrov-Kazakov v. Bulgaria Shimovolos v. Russia Khellil v. Switzerland M.M. v. the United Kingdom M.K. v. France Peruzzo and Martens v. Germany Brunet v. France Figueiredo Teixeira v. Andorra Dagregorio and Mosconi v. France Aycaguer v. France López Ribalda v. Spain, and Gancedo Giménez and Others v. Spain PENDING Catt v. the United Kingdom PENDING Chave née Julien v. France L.L. v. France Vukota-Bojic v. Switzerland Leander v. Sweden Rotaru v. Romania Turek v. Slovakia Breyer v. Germany PENDING Čalović v. Montenegro PENDING Z. v. Finland M.S. v. Sweden (no. 20837/92) Peck v. the United Kingdom Pantelyeyenko v. Ukraine Armonas v. Lithuania and Birlik v. Lithuania Avilkina and Others v. Russia Radu v. the Republic of Moldova Sõro v. Estonia Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland Gaskin v. the United Kingdom Odievre v. France Roche v. the United Kingdom Segerstedt-Wiberg and Others v. Sweden K.H. and Others v. Slovakia Haralambie v. Romania Godelli v. Italy Magyar Helsinki Bizottság v. Hungary	02/09/2010 03/02/2012 29/04/2014 06/09/1978 02/08/1984 24/04/1990 25/03/1998 16/02/2000 22/10/2002 22/12/2004 18/05/2010 15/01/2015 27/10/2015 04/12/2015 12/01/2016 21/11/2011 06/05/2013 09/01/2014 05/01/2015 24/11/2015 12/01/2016 30/03/2012 25/09/2001 31/05/2015 28/01/2003 05/10/2010 03/12/2014 17/07/2003 04/12/2008 17/12/2009 10/02/2011 21/06/2011 18/10/2011 13/11/2012 18/04/2013 04/06/2013 18/09/2014 08/11/2016 30/05/2017 22/06/2017 17/02/2015 19/05/2016 09/07/1991 10/10/2006 18/10/2016 23/03/1987 04/05/2000 14/02/2006 21/03/2016 31/03/2016 25/02/1997 27/02/1997 28/01/2003 29/06/2006 25/11/2008 06/06/2013 15/03/2014 03/09/2015 27/06/2017 07/07/1989 13/02/2003 19/10/2005 06/06/2006 28/06/2009 27/10/2009 25/09/2012 08/11/2016	COLLECTION ON PERSONAL DATA: GPS data + STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice COLLECTION ON PERSONAL DATA: GPS data COLLECTION ON PERSONAL DATA: Health data COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance COLLECTION ON PERSONAL DATA: Monitoring of employees' computer use COLLECTION ON PERSONAL DATA: Monitoring of employees' computer use COLLECTION ON PERSONAL DATA: Voice samples COLLECTION ON PERSONAL DATA: Voice samples COLLECTION ON PERSONAL DATA: Video surveillance + DISCLOSURE OF PERSONAL DATA COLLECTION ON PERSONAL DATA: Video surveillance COLLECTION ON PERSONAL DATA: Video surveillance STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice STORAGE AND USE OF PERSONAL DATA: In	

Robathin v. Austria	03/07/2012	ELECTRONIC DATA	violation of Article 8
Bernh Larsen Holding As and Others v. Norway	14/03/2013	ELECTRONIC DATA	no violation of Article 8
M.K. v. France	18/04/2013	ELECTRONIC DATA	violation of Article 8
Youth Initiative For Human Rights v. Serbia	25/06/2013	ELECTRONIC DATA	violation of Article 10
Nagla v. Latvia	16/07/2013	ELECTRONIC DATA	violation of Article 10
Peruzzo and Martens v. Germany	04/06/2013	ELECTRONIC DATA	inadmissible
Brunet v. France	18/09/2014	ELECTRONIC DATA	violation of Article 8
Sérvulo & Associados - Sociedade de Advogados, RL v. Portugal	03/09/2015	ELECTRONIC DATA	no violation of Article 8
Szabó and Vissy v. Hungary	12/01/2016	ELECTRONIC DATA	violation of Article 8, no violation of Article 13
Trabajo Rueda v. Spain	30/05/2017	ELECTRONIC DATA	violation of Article 8
Dagregorio and Mosconi v. France	30/05/2017	ELECTRONIC DATA	inadmissible
Aycaguer v. France	22/06/2017	ELECTRONIC DATA	violation of Article 8
Centrum För Rättvisa v. Sweden PENDING	21/11/2011	ELECTRONIC DATA	Articles 8 (right to respect for private life), 13 (right to an effective remedy) and 34 (individual applications) of the Convention.
Ivashchenko v. Russia PENDING	05/10/2011	ELECTRONIC DATA	Articles 8 (right to respect for private life and correspondence), 10 (freedom of expression) and 13 (right to an effective remedy) of the Convention.
Tretter and Others v. Austria PENDING	06/05/2013	ELECTRONIC DATA	Articles 34 (right of individual petition), 8 (right to respect for private life and correspondence) and 10 (freedom of expression) of the Convention.
Libert v. France PENDING	30/03/2015	ELECTRONIC DATA	Article 8 (right to respect for private life) of the Conventi
Big Brother Watch and Others v. the United Kingdom PENDING	09/01/2014	ELECTRONIC DATA	Article 8 (right to respect for private life) of the Convention.
Bureau of Investigative Journalism and Alice Ross v. the United Kingdom PENDING	05/01/2015	ELECTRONIC DATA	Articles 8 (right to respect for private life) and 10 (freedom of expression) of the Convention.
Association confraternelle de la presse judiciaire v. France et 11 autres requêtes	26/04/2017	ELECTRONIC DATA	Article 8 (right to respect for private life) of the Convention.
Catt v. the United Kingdom	19/05/2016	ELECTRONIC DATA	Article 8 (right to respect for private life) of the Convention.
Copland v. the United Kingdom	03/04/2007	EMAIL	violation of Article 8
Muscio v. Italy	13/11/2007	EMAIL	inadmissible. Art. 8
Benediktsdóttir v. Iceland	16/06/2009	EMAIL	inadmissible. Art. 8
Helander v. Finland	10/09/2013	EMAIL	inadmissible
Sérvulo & Associados - Sociedade de Advogados, RL v. Portugal	03/09/2015	EMAIL	no violation of Article 8
Uzun v. Germany	02/09/2010	GPS (Global Positioning System)	no violation of Article 8
Ben Faiza v. France PENDING	03/02/2015	GPS (Global Positioning System)	Article 8 (right to respect for private life) of the Convention.
Perrin v. the United Kingdom	18/10/2005	INTERNET	inadmissible. Art. 10
Paeffgen GmbH v. Germany	18/09/2007	INTERNET	inadmissible. Article 1 (protection of property) of Protocol No. 1 to the Convention.
K.U. v. Finland	02/12/2008	INTERNET	violation of Article 8
Times Newspapers Ltd v. the United Kingdom	10/03/2009	INTERNET	no violation of Article 10
Willem v. France	16/07/2009	INTERNET	no violation of Article 10
Renaud v. France	25/02/2010	INTERNET	violation of Article 10
Editorial Board of Pravoye Delo and Shtekel v. Ukraine	05/05/2011	INTERNET	violation of Article 10
Mosley v. the United Kingdom	10/05/2011	INTERNET	no violation of Article 8
Ahmet Yildirim v. Turkey	18/12/2012	INTERNET	violation of Article 10
Ashby Donald and Others v. France	10/01/2013	INTERNET	no violation of Article 10
Neij and Sunde Kolmisoppi v. Sweden	19/02/2013	INTERNET	inadmissible. Art. 10
Akdeniz v. Turkey	11/03/2014	INTERNET	inadmissible. Art. 34
Delfi AS v. Estonia	16/06/2015	INTERNET	no violation of Article 10
Cengiz and Others v. Turkey	01/12/2015	INTERNET	violation of Article 10
Kalda v. Estonia	19/01/2016	INTERNET	violation of Article 10
Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary	02/02/2016	INTERNET	violation of Article 10
Dallas v. the United Kingdom	11/02/2016	INTERNET	no violation of Article 7
Pihl v. Sweden	07/02/2017	INTERNET	inadmissible
Bărbulescu v. Romania PENDING	12/01/2016	INTERNET	no violation of Article 8
M.L. v. Germany and W.W. v. Germany PENDING	28/11/2012	INTERNET	Article 8 (right to respect for private life) of the Convention.
Kharitonov v. Russia PENDING	27/04/2017	INTERNET	Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention.
SIA AKKA/LAA v. Latvia	12/07/2016	MUSICAL COPYRIGHT	no violation of Article 1 (protection of property) of Protocol No. 1 to the Convention and no violation of Article 6 § 1 (right to fair trial) of the Convention.
Brambilla and Others v. Italy	23/06/2016	RADIO COMMUNICATIONS	no violation of Article 10
Khurshid Mustafa and Tarzibachi v. Sweden	16/12/2008	SATELLITE DISH	violation of Article 10
Roman Zakharov v. Russia	04/12/2015	TELECOMMUNICATIONS	violation of Article 8
Breyer v. Germany PENDING	21/03/2016	TELECOMMUNICATIONS	Articles 8 (right to respect for private life and correspondence) and 10 (freedom of expression) of the Convention.
Čalović v. Montenegro	31/03/2016	TELECOMMUNICATIONS	Articles 8 (right to respect for private life), 34 (individual applications) and 35 (admissibility criteria) of the Convention.
Haldimann and Others v. Switzerland	24/02/2015	USE OF HIDDEN CAMERAS	violation of Article 10
Bremner v. Turkey	13/10/2015	USE OF HIDDEN CAMERAS	violation of Article 8
Peck v. the United Kingdom	28/01/2003	VIDEO SURVEILLANCE	violation of Article 8 and 13
Perry v. the United Kingdom	17/07/2003	VIDEO SURVEILLANCE	violation of Article 8
Köpke v. Germany	05/10/2010	VIDEO SURVEILLANCE	inadmissible. Art. 8
Riina v. Italy	11/03/2014	VIDEO SURVEILLANCE	inadmissible. Articles 3 (prohibition of inhuman or degrading treatment) and 8 (right to respect for private and family life) of the Convention
Vasilică Mocanu v. Romania	06/12/2016	VIDEO SURVEILLANCE	violation of Article 8
Antović and Mirković v. Montenegro PENDING	03/12/2014	VIDEO SURVEILLANCE	Articles 8 (right to respect for private life) and 35 (admissibility criteria) of the Convention.
López Ribalda v. Spain , and Gancedo Giménez and Others v. Spain PENDING	17/02/2015	VIDEO SURVEILLANCE	Articles 6 (right to a fair trial) and 8 (right to respect for private life) of the Convention.
FACTSHEET: MASS SURVEILLANCE			
Klass and Others v. Germany	06/09/1978	MASS SURVEILLANCE	no violation of Article 8
Weber and Saravia v. Germany	29/06/2006	MASS SURVEILLANCE	inadmissible
Liberty and Others v. the United Kingdom	01/07/2008	MASS SURVEILLANCE	violation of Article 8
Kennedy v. the United Kingdom	18/05/2010	MASS SURVEILLANCE	no violation of Article 8
Roman Zakharov v. Russia	04/12/2015	MASS SURVEILLANCE	violation of Article 8
Szabó and Vissy v. Hungary	12/01/2016	MASS SURVEILLANCE	violation of Article 8, no violation of Article 13
Centrum För Rättvisa v. Sweden PENDING	21/11/2011	MASS SURVEILLANCE	Articles 8 (right to respect for private life), 13 (right to an effective remedy) and 34 (individual applications) of the Convention.
Tretter and Others v. Austria PENDING	06/05/2013	MASS SURVEILLANCE	Articles 34 (right of individual petition), 8 (right to respect for private life and correspondence) and 10 (freedom of expression) of the Convention.
Big Brother Watch and Others v. the United Kingdom PENDING	09/01/2014	MASS SURVEILLANCE	Article 8 (right to respect for private life) of the Convention.
Bureau of Investigative Journalism and Alice Ross v. the United Kingdom PENDING	05/01/2015	MASS SURVEILLANCE	Articles 8 (right to respect for private life) and 10 (freedom of expression) of the Convention.
10 Human Rights Organisations and Others v. the United Kingdom PENDING	24/11/2015	MASS SURVEILLANCE	Articles 6 § 1 (right to a fair trial), 8 (right to respect for private life), 10(freedom of expression), 14 (prohibition of discrimination) and 34 (individual applications) of the Convention.

Association confraternelle de la presse judiciaire v. France et 11 autres requêtes PENDING	26/04/2017	MASS SURVEILLANCE	Article 8 (right to respect for private life and correspondence), Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention.
HANDBOOK ON DATA PROTECTION			
Allan v. the United Kingdom	05/11/2002	SURVEILLANCE METHODS	violation of Article 8
Association "21 Decembrie 1989" and Others v. Romania	24/05/2011	SURVEILLANCE METHODS	violation of Article 8
Association for European Integration and Human Rights and Ekimdzhiiev v. Bulgaria	28/06/2007	SURVEILLANCE METHODS	violation of Article 8 and 13, no violation of article 6
Axel Springer AG v. Germany	07/02/2012	FREEDOM OF PRESS	violation of Article 10
Bykov v. Russia	10/03/2009	SURVEILLANCE METHODS	violation of Article 8 and 5.3, no violation of article 6
Cemalettin Canli v. Turkey	18/11/2008	CORRESPONDENCE	violation of Article 8
Clubotaru v. Moldova,	27/10/2010	IDENTITY	violation of Article 8
Cotlet v. Romania	03/06/2003	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
Dalea v. France	02/02/2010	CORRESPONDENCE	no violation of Article 8
Halford v. the United Kingdom	25/06/1997	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8 and 13
I. v. Finland	17/07/2008	ACCESS TO PERSONAL DATA	violation of Article 8
Iordachi and Others v. Moldova	10/02/2009	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8, no violation of Article 13
Kennedy v. the United Kingdom	18/05/2010	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	no violation of Article 8, 13 and 6.1
Köpke v. Germany	05/10/2010	VIDEO SURVEILLANCE	no violation of Article 8, inadmissible
Lambert v. France	24/08/1998	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
M.G. v. the United Kingdom	24/09/2002	CORRESPONDENCE	violation of Article 8
McMichael v. the United Kingdom	24/02/1995	CORRESPONDENCE	violation of Article 8 and 6
Michaud v. France	06/12/2012	CORRESPONDENCE. INFORMATION CONCERNING PROFESSIONAL ACTIVITIES	no violation of Article 8
Müller and Others v. Switzerland	24/05/1998	FREEDOM OF ARTS	no violation of Article 10
Niemietz v. Germany	16/12/1992	CORRESPONDENCE. INFORMATION CONCERNING PROFESSIONAL ACTIVITIES	violation of Article 8
Odibvre v. France	13/02/2003	ACCESS TO PERSONAL DATA	no violation of Article 8
Sciaccia v. Italy	11/01/2005	PHOTOS	violation of Article 8
Silver and Others v. the United Kingdom	25/03/1993	CORRESPONDENCE	violation of Article 8, 13 and 6, no violation of article 10
Szuluk v. the United Kingdom	02/06/2009	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
Társaság a Szabadságjogokért v. Hungary	14/04/2009	ACCESS TO INFORMATION	violation of Article 10
The Sunday Times v. the United Kingdom	26/04/1979	FREEDOM OF PRESS	violation of Article 10, no violation of article 14
Vereinigung bildender Künstler v. Austria	25/01/2007	FREEDOM OF ARTS	violation of Article 10
Von Hannover v. Germany	07/02/2012	PHOTOS	no violation of Article 8
Von Hannover v. German	24/06/2004	PHOTOS	violation of Article 10

Anexo 2. La Jurisprudencia del TEDH en materia de protección de datos: orden cronológico

Etiquetas de fila

06/09/1978	Klass and Others v. Germany	MASS SURVEILLANCE	no violation of Article 8
	Klass and Others v. Germany	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	no violation of Article 8
26/04/1979	The Sunday Times v. the United Kingdom	FREEDOM OF PRESS	violation of Article 10, no violation of article 14
25/03/1983	Silver and Others v. the United Kingdom	CORRESPONDENCE	violation of Article 8, 13 and 6, no violation of article 10
02/08/1984	Malone v. the United Kingdom	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
23/03/1987	Leander v. Sweden	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers	no violation of Article 8
07/07/1989	Gaskin v. the United Kingdom	ACCESS TO PERSONAL DATA	violation of Article 8
24/04/1990	Kruslin v. France	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
09/07/1991	Chave née Jullien v. France	STORAGE AND USE OF PERSONAL DATA: In the context of health	inadmissible
16/12/1992	Niemietz v. Germany	CORRESPONDENCE. INFORMATION CONCERNING PROFESSIONAL ACTIVITIES	violation of Article 10
24/02/1995	McMichael v. the United Kingdom	CORRESPONDENCE	violation of Article 8 and 6
25/02/1997	Z. v. Finland (no. 22009/93)	DISCLOSURE OF PERSONAL DATA	violation of Article 8
27/02/1997	M.S. v. Sweden (no. 20837/92)	DISCLOSURE OF PERSONAL DATA	no violation of Article 8
25/06/1997	Halford v. the United Kingdom	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8 and 13
25/03/1998	Kopp v. Switzerland	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
24/05/1998	Müller and Others v. Switzerland	FREEDOM OF ARTS	no violation of Article 10
24/08/1998	Lambert v. France	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
16/02/2000	Amann v. Switzerland	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
04/05/2000	Rotaru v. Romania	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers + ERASURE OR DESTRUCTION OF PERSONAL DATA	violation of Article 8 and 13
25/09/2001	P.G. and J.H. v. the United Kingdom	COLLECTION ON PERSONAL DATA: Voice samples	violation of Article 8, no violation of Article 8
24/09/2002	M.G. v. the United Kingdom	CORRESPONDENCE	violation of Article 8
22/10/2002	Taylor-Sabori v. the United Kingdom	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8
05/11/2002	Allan v. the United Kingdom	SURVEILLANCE METHODS	

	violation of Article 8
28/01/2003	Peck v. the United Kingdom
	COLLECTION ON PERSONAL DATA: Video surveillance + DISCLOSURE OF PERSONAL DATA
	in breach of Article 8
	DISCLOSURE OF PERSONAL DATA
	violation of Article 8 and 13
	VIDEO SURVEILLANCE
	violation of Article 8 and 13
13/02/2003	Odièvre v. France
	ACCESS TO PERSONAL DATA
	no violation of Article 8
03/06/2003	Cotlet v. Romania
	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
	violation of Article 8
17/07/2003	Perry v. the United Kingdom
	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
	violation of Article 8
	VIDEO SURVEILLANCE
	violation of Article 8
24/06/2004	Von Hannover v. German
	PHOTOS
	violation of Article 10
11/01/2005	Sciacca v. Italy
	PHOTOS
	violation of Article 8
18/10/2005	Perrin v. the United Kingdom
	INTERNET
	Inadmissible. Art. 10
19/10/2005	Roche v. the United Kingdom
	ACCESS TO PERSONAL DATA
	violation of Article 8
22/12/2005	Wisse v. France
	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
	violation of Article 8
14/02/2006	Turek v. Slovakia
	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers + ACCESS TO PERSONAL DATA
	violation of Article 8
06/06/2006	Segerstedt-Wiberg and Others v. Sweden
	ACCESS TO PERSONAL DATA
	no violation of Article 8
29/06/2006	Panteleyenko v. Ukraine
	DISCLOSURE OF PERSONAL DATA
	violation of Article 8
	Weber and Saravia v. Germany
	MASS SURVEILLANCE
	inadmissible
10/10/2006	L.L. v. France
	STORAGE AND USE OF PERSONAL DATA: In the context of health
	violation of Article 8
25/01/2007	Vereinigung bildender Künstler v. Austria
	FREEDOM OF ARTS
	violation of Article 10
03/04/2007	Copland v. the United Kingdom
	EMAIL
	violation of Article 8
28/06/2007	Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria
	SURVEILLANCE METHODS
	violation of Article 8 and 13, no violation of article 6
18/09/2007	Paefgen GmbH v. Germany
	INTERNET
	inadmissible. Article 1 (protection of property) of Protocol No. 1 to the Convention.
13/11/2007	Muscio v. Italy
	EMAIL
	Inadmissible. Art. 8
01/07/2008	Liberty and Others v. the United Kingdom
	MASS SURVEILLANCE
	violation of Article 8
17/07/2008	I. v. Finland
	ACCES TO PERSONAL DATA
	violation of Article 8
18/11/2008	Cemalettin Canli v. Turkey

	CORRESPONDENCE
	violation of Article 8
25/11/2008	
	Armonas v. Lithuania and Biriuk v. Lithuania
	DISCLOSURE OF PERSONAL DATA
	violation of Article 8
02/12/2008	
	K.U. v. Finland
	INTERNET
	violation of Article 8
04/12/2008	
	S. and Marper v. the United Kingdom
	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
	violation of Article 8
	S. and Marper v. the United Kingdom
	ELECTRONIC DATA
	violation of Article 8
16/12/2008	
	Khurshid Mustafa and Tarzibachi v. Sweden
	SATELLITE DISH
	violation of Article 10
10/02/2009	
	Iordachi and Others v. Moldova
	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
	violation of Article 8, no violation of Article 13
10/03/2009	
	Bykov v. Russia
	SURVEILLANCE METHODS
	violation of Article 8 and 5.3, no violation of article 6
	Times Newspapers Ltd v. the United Kingdom
	INTERNET
	no violation of Article 10
14/04/2009	
	Társaság a Szabadságjogokért v. Hungary
	ACCESS TO INFORMATION
	violation of Article 10
02/06/2009	
	Szuluk v. the United Kingdom
	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
	violation of Article 8
16/06/2009	
	Benediktsdóttir v. Iceland
	EMAIL
	Inadmissible. Art. 8
28/06/2009	
	K.H. and Others v. Slovakia
	ACCESS TO PERSONAL DATA
	violation of Article 8
16/07/2009	
	Willem v. France
	INTERNET
	no violation of Article 10
27/10/2009	
	Haralambie v. Romania
	ACCESS TO PERSONAL DATA
	violation of Article 8
17/12/2009	
	B.B. v. France , Gardel v. France and M.B. v. France
	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
	no violation of Article 8
	B.B. v. France, Gardel v. France and M.B. v. France
	ELECTRONIC DATA
	no violation of Article 8
02/02/2010	
	Dalea v. France
	CORRESPONDENCE
	no violation of Article 8
25/02/2010	
	Renaud v. France
	INTERNET
	violation of Article 10
18/05/2010	
	Kennedy v. the United Kingdom
	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
	no violation of Article 8
	MASS SURVEILLANCE
	no violation of Article 8
	Kennedy v. the United Kingdom
	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
	no violation of Article 8 , 13 and 6.1
02/09/2010	
	Uzun v. Germany
	GPS (Global Positioning System)
	no violation of Article 8
	Uzun v. Germany
	COLLECTION ON PERSONAL DATA: GPS data + STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
	no violation of Article 8
05/10/2010	
	Köpke v. Germany
	COLLECTION ON PERSONAL DATA: Video surveillance
	Inadmissible. Art. 8
	VIDEO SURVEILLANCE

	Inadmissible. Art. 8 no violation of Article 8, inadmissible
27/10/2010	Ciubotaru v. Moldova, IDENTITY violation of Article 8
10/02/2011	Dimitrov-Kazakov v. Bulgaria STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice violation of Article 8 and 13
05/05/2011	Editorial Board of Pravoye Delo and Shtekel v. Ukraine INTERNET violation of Article 10
10/05/2011	Mosley v. the United Kingdom INTERNET no violation of Article 8
24/05/2011	Association "21 Décembre 1989" and Others v. Romania SURVEILLANCE METHODS violation of Article 8
21/06/2011	Shimovolos v. Russia STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice violation of Article 8 Shimovolos v. Russia ELECTRONIC DATA violation of Article 8 and 5
05/10/2011	Ivashchenko v. Russia PENDING ELECTRONIC DATA Articles 8 (right to respect for private life and correspondence), 10 (freedom of expression) and 13 (right to an effective remedy) of the Convention.
18/10/2011	Khelili v. Switzerland STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice violation of Article 8
13/11/2011	Mandil v. France, Barreau and Others v. France and Deceuninck v. France ELECTRONIC DATA inadmissible
21/11/2011	Centrum För Rättvisa v. Sweden PENDING COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance Articles 8 (right to respect for private life), 13 (right to an effective remedy) and 34 (individual applications) of the Convention ELECTRONIC DATA Articles 8 (right to respect for private life), 13 (right to an effective remedy) and 34 (individual applications) of the Convention. MASS SURVEILLANCE Articles 8 (right to respect for private life), 13 (right to an effective remedy) and 34 (individual applications) of the Convention.
03/02/2012	Ben Faiza v. France PENDING COLLECTION ON PERSONAL DATA: GPS data violation of Article 8?
07/02/2012	Axel Springer AG v. Germany FREEDOM OF PRESS violation of Article 10 Von Hannover v. Germany PHOTOS no violation of Article 8
30/03/2012	Libert v. France PENDING COLLECTION ON PERSONAL DATA: Monitoring of employees' computer use Article 8 (right to respect for private life)
03/07/2012	Robathin v. Austria ELECTRONIC DATA violation of Article 8
25/09/2012	Godelli v. Italy ACCESS TO PERSONAL DATA violation of Article 8
13/11/2012	M.M. v. the United Kingdom STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice violation of Article 8
28/11/2012	M.L. v. Germany and W.W. v. Germany PENDING INTERNET Article 8 (right to respect for private life) of the Convention.
06/12/2012	Michaud v. France CORRESPONDENCE. INFORMATION CONCERNING PROFESSIONAL ACTIVITIES no violation of Article 8
18/12/2012	Ahmet Yıldırım v. Turkey INTERNET violation of Article 10
10/01/2013	Ashby Donald and Others v. France INTERNET no violation of Article 10

19/02/2013
Neij and Sunde Kolmisoppi v. Sweden
INTERNET
Inadmissible. Art. 10
14/03/2013
Bernh Larsen Holding As and Others v. Norway
ELECTRONIC DATA
no violation of Article 8
18/04/2013
M.K. v. France
ELECTRONIC DATA
violation of Article 8
STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
violation of Article 8
06/05/2013
Tretter and Others v. Austria PENDING
COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
Articles 34 (right of individual petition), 8 (right to respect for private life and correspondence) and 10 (freedom of expression) of the Convention
ELECTRONIC DATA
Articles 34 (right of individual petition), 8 (right to respect for private life and correspondence) and 10 (freedom of expression) of the Convention.
MASS SURVEILLANCE
Articles 34 (right of individual petition), 8 (right to respect for private life and correspondence) and 10 (freedom of expression) of the Convention.
04/06/2013
Peruzzo and Martens v. Germany
ELECTRONIC DATA
inadmissible
STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
inadmissible
06/06/2013
Avilkina and Others v. Russia
DISCLOSURE OF PERSONAL DATA
violation of Article 8
25/06/2013
Youth Initiative For Human Rights v. Serbia
ELECTRONIC DATA
violation of Article 10
16/07/2013
Nagla v. Latvia
ELECTRONIC DATA
violation of Article 10
10/09/2013
Helander v. Finland
EMAIL
inadmissible
09/01/2014
Big Brother Watch and Others v. the United Kingdom PENDING
COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
Article 8 (right to respect for private life) of the Convention
ELECTRONIC DATA
Article 8 (right to respect for private life) of the Convention.
MASS SURVEILLANCE
Article 8 (right to respect for private life) of the Convention.
11/03/2014
Akdeniz v. Turkey
INTERNET
inadmissible. Art. 34
Riina v. Italy
VIDEO SURVEILLANCE
inadmissible. Articles 3 (prohibition of inhuman or degrading treatment) and 8 (right to respect for private and family life) of the Convention
15/03/2014
Radu v. the Republic of Moldova
DISCLOSURE OF PERSONAL DATA
violation of Article 8
29/04/2014
L.H. v. Latvia
COLLECTION ON PERSONAL DATA: Health data
violation of Article 8
18/09/2014
Brunet v. France
ELECTRONIC DATA
violation of Article 8
STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
violation of Article 8
03/12/2014
Antović and Mirković v. Montenegro PENDING
COLLECTION ON PERSONAL DATA: Video surveillance
Articles 8 (right to respect for private life) and 35 (admissibility criteria) of the Convention
VIDEO SURVEILLANCE
Articles 8 (right to respect for private life) and 35 (admissibility criteria) of the Convention.
05/01/2015
Bureau of Investigative Journalism and Alice Ross v. the United Kingdom PENDING
COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
Articles 8 (right to respect for private life) and 10 (freedom of expression) of the Convention.
ELECTRONIC DATA
Articles 8 (right to respect for private life) and 10 (freedom of expression) of the Convention.
MASS SURVEILLANCE
Articles 8 (right to respect for private life) and 10 (freedom of expression) of the Convention.
15/01/2015
Dragojević v. Croatia
COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
violation of Article 8
03/02/2015

Ben Faiza v. France PENDING
GPS (Global Positioning System)
Article 8 (right to respect for private life) of the Convention.
17/02/2015
López Ribalda v. Spain , and Gancedo Giménez and Others v. Spain PENDING
STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
Articles 6 (right to a fair trial) and 8 (right to respect for private life) of the Convention.
VIDEO SURVEILLANCE
Articles 6 (right to a fair trial) and 8 (right to respect for private life) of the Convention.
24/02/2015
Haldimann and Others v. Switzerland
USE OF HIDDEN CAMERAS
violation of Article 10
30/03/2015
Libert v. France PENDING
ELECTRONIC DATA
Article 8 (right to respect for private life) of the Conventi
31/05/2015
Vetter v. France
COLLECTION ON PERSONAL DATA: Voice samples
violation of Article 8
16/06/2015
Delfi AS v. Estonia
INTERNET
no violation of Article 10
03/09/2015
Sérvulo & Associados - Sociedade de Advogados, RL v. Portugal
ELECTRONIC DATA
no violation of Article 8
EMAIL
no violation of Article 8
Sõro v. Estonia
DISCLOSURE OF PERSONAL DATA
violation of Article 8
13/10/2015
Bremner v. Turkey
USE OF HIDDEN CAMERAS
violation of Article 8
27/10/2015
R.E. v. the United Kingdom (no. 62498/11)
COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
violation of Article 8, no violation of Article 8
24/11/2015
10 Human Rights Organisations and Others v. the United Kingdom PENDING
COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
Articles 6 § 1 (right to a fair trial), 8 (right to respect for private life), 10(freedom of expression), 14 (prohibition of discrimination) and 34 (individual applications) of the Convention
MASS SURVEILLANCE
Articles 6 § 1 (right to a fair trial), 8 (right to respect for private life), 10(freedom of expression), 14 (prohibition of discrimination) and 34 (individual applications) of the Convention.
01/12/2015
Cengiz and Others v. Turkey
INTERNET
violation of Article 10
04/12/2015
Roman Zakharov v. Russia
COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
violation of Article 8
MASS SURVEILLANCE
violation of Article 8
TELECOMMUNICATIONS
violation of Article 8
12/01/2016
Bărbulescu v. Romania PENDING
INTERNET
no violation of Article 8
Bărbulescu v. Romania PENDING
COLLECTION ON PERSONAL DATA: Monitoring of employees' computer use
no violation of Article 8
Szabó and Vissy v. Hungary
COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance
violation of Article 8
MASS SURVEILLANCE
violation of Article 8, no violation of Article 13
Szabó and Vissy v. Hungary
ELECTRONIC DATA
violation of Article 8, no violation of Article 13
19/01/2016
Kalda v. Estonia
INTERNET
violation of Article 10
02/02/2016
Magyar Tartalomsgéltatók Egyesülete and Index.hu Zrt v. Hungary
INTERNET
violation of Article 10
11/02/2016
Dallas v. the United Kingdom
INTERNET
no violation of Article 7
21/03/2016
Breyer v. Germany PENDING
STORAGE AND USE OF PERSONAL DATA: Telecommunication service providers' data
Articles 8 (right to respect for private life and correspondence) and 10 (freedom of expression)
TELECOMMUNICATIONS

Articles 8 (right to respect for private life and correspondence) and 10 (freedom of expression) of the Convention.	
31/03/2016	Čalović v. Montenegro
	TELECOMMUNICATIONS
	Articles 8 (right to respect for private life), 34 (individual applications) and 35 (admissibility criteria) of the Convention.
	Čalović v. Montenegro PENDING
	STORAGE AND USE OF PERSONAL DATA: Telecommunication service providers' data
	Articles 8 (right to respect for private life), 34 (individual applications) and 35 (admissibility criteria) of the Convention.
19/05/2016	Catt v. the United Kingdom
	ELECTRONIC DATA
	Article 8 (right to respect for private life) of the Convention.
	Catt v. the United Kingdom PENDING
	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
	Article 8 (right to respect for private life)
23/06/2016	Brambilla and Others v. Italy
	RADIO COMMUNICATIONS
	no violation of Article 10
12/07/2016	SIA AKKA/LAA v. Latvia
	MUSICAL COPYRIGHT
	no violation of Article 1 (protection of property) of Protocol No. 1 to the Convention and no violation of Article 6 § 1 (right to fair trial) of the Convention.
18/10/2016	Vukota-Bojic v. Switzerland
	STORAGE AND USE OF PERSONAL DATA: In social insurance proceedings
	violation of Article 8
08/11/2016	Figueiredo Teixeira v. Andorra
	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
	no violation of Article 8
	Magyar Helsinki Bizottság v. Hungary
	ACCESS TO PERSONAL DATA
	violation of Article 10
06/12/2016	Vasilică Mocanu v. Romania
	VIDEO SURVEILLANCE
	violation of Article 8
07/02/2017	Pihl v. Sweden
	INTERNET
	inadmissible
26/04/2017	Association confraternelle de la presse judiciaire v. France et 11 autres requêtes
	ELECTRONIC DATA
	Article 8 (right to respect for private life and correspondence), Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention.
	Association confraternelle de la presse judiciaire v. France et 11 autres requêtes PENDING
	MASS SURVEILLANCE
	Article 8 (right to respect for private life and correspondence), Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention.
27/04/2017	Kharitonov v. Russia PENDING
	INTERNET
	Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention.
30/05/2017	Dagregorio and Mosconi v. France
	ELECTRONIC DATA
	inadmissible
	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
	inadmissible
	Trabajo Rueda v. Spain
	ELECTRONIC DATA
	violation of Article 8
22/06/2017	Aycaguer v. France
	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice
	violation of Article 8
	Aycaguer v. France
	ELECTRONIC DATA
	violation of Article 8
27/06/2017	Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland
	DISCLOSURE OF PERSONAL DATA
	no violation of Article 10
	(vacío)

Total general

STATUS: lunes 17 de julio de 2017

Anexo 3. La Jurisprudencia del TEDH en materia de protección de datos: datos cualitativos y cuantitativos por décadas					
DÉCADAS	Nº CASOS	Nº CASOS ART.8	TEMÁTICA	ARTÍCULOS EN CUESTIÓN	OBSERVACIONES
1970-1979	2	1	MASS SURVEILLANCE, COLLECTION (interception of communications, phone tapping and secret surveillance), FREEDOM OF PRESS	8, 10	Sin presencia de las nuevas tecnologías
1980-1989	4	4	COLLECTION (interception of communications(...), correspondence), STORAGE AND USE (secret registers), ACCESS	8, 10, 13, 6	Art. 6 y 13 con presencia residual
1990-1999	10	7	COLLECTION (interception of communications, correspondence), STORAGE AND USE (health), DISCLOSURE , FREEDOM OF ARTS	8, 10, 6	Art. 10 y 6 con presencia residual
2000-2009	42	34	COLLECTION (interception of communications(...), correspondence, monitoring of employee's computer use , health data, voice samples), STORAGE AND USE (secret registers, criminal justice , health), ERASURE OR DESTRUCTION , VIDEO SURVEILLANCE , SURVEILLANCE METHODS , MASS SURVEILLANCE , PHOTOS , DISCLOSURE , INTERNET , ACCES , MASS SURVEILLANCE , EMAIL , ELECTRONIC DATA , SATELLITE DISH , FREEDOM OF ARTS	art.1 y Protocolo Nº1, 6, (casos aislados), 8 y 10 (fundamentalmente, a veces acompañando al art.8 el art. 13)	Aparecen la mayoría de las nuevas temáticas, numerosos casos vulnerados simultáneamente bajo varias temáticas
2010-2017	77	52	COLLECTION (interception of communications(...), correspondence, GPS data , monitoring of employee's computer use, health data, voice samples), STORAGE AND USE (secret registers, criminal justice, health, in social insurance proceedings , telecommunication service provider's data), IDENTITY , ERASURE OR DESTRUCTION , VIDEO SURVEILLANCE , DISCLOSURE , INTERNET , PHOTOS , ACCES , MASS SURVEILLANCE , EMAIL , ELECTRONIC DATA , SATELLITE DISH , RADIO COMMUNICATIONS , USE OF HIDDEN CAMERAS , TELECOMMUNICATIONS , RADIO COMMUNICATIONS , MUSICAL COPYRIGHT , FREEDOM OF PRESS	art.1 y Protocolo Nº1, 6.1, 7, 5 (casos aislados), 8 y 10 (fundamentalmente, a veces acompañando al art. 8 los art.s 13, 34 ó 35)	Aparecen algunas nuevas temáticas, los casos de Internet y Electronic data crecen en número de casos así, como las vulneraciones de los arts. 10 y 13. Se vulneran varios artículos simultáneamente, y las sentencias recaen sobre varias temáticas simultáneamente.

Anexo 4. La Jurisprudencia del TEDH en materia de protección de datos: contenido del derecho				
Amann v. Switzerland	16/02/2000	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	No separation between matters of private and professional life ; para. 65. It points out in this connection that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life".
P.G. and J.H. v. the United Kingdom	25/09/2001	COLLECTION ON PERSONAL DATA: Voice samples	violation of Article 8, no violation of Article 8	Personal data as sound ; para 59 y 60. The Court's case-law has, on numerous occasions, found that the covert taping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed. While it is generally the case that the recordings were made for the purpose of using the content of the conversations in some way, the Court is not persuaded that recordings taken for use as voice samples can be regarded as falling outside the scope of the protection afforded by Article 8. A permanent record has nonetheless been made of the person's voice and it is subject to a process of analysis directly relevant to identifying that person in the context of other personal data. Though it is true that when being charged the applicants answered formal questions in a place where police officers were listening to them, the recording and analysis of their voices on this occasion must still be regarded as concerning the processing of personal data about the applicants. The Court concludes therefore that the recording of the applicants' voices when being charged and when in their police cell discloses an interference with their right to respect for private life within the meaning of Article 8 § 1 of the Convention / other elements as gender, name, sexual orientation and sexual life, some interaction in a public context, also fall into a personal sphere.
Peck v. the United Kingdom	28/01/2003	COLLECTION ON PERSONAL DATA: Video surveillance + DISCLOSURE OF PERSONAL DATA	in breach of Article 8	Personal data by footage and disclosure of video surveillance ; para 85. In sum, the Court does not find that, in the circumstances of this case, there were relevant or sufficient reasons which would justify the direct disclosure by the Council to the public of stills from the footage in its own CCTV News article without the Council obtaining the applicant's consent or masking his identity, or which would justify its disclosures to the media without the Council taking steps to ensure so far as possible that such masking would be effected by the media. The crime-prevention objective and context of the disclosures demanded particular scrutiny and care in these respects in the present case.
S. and Marper v. the United Kingdom	04/12/2008	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice + ELECTRONIC DATA	violation of Article 8	Personal data by different elements ; para 66. Personal data by DNA, fingerprints and cellular samples; para 68. The Court notes that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (see Pretty v. the United Kingdom, no. 2346/02, § 61, ECHR 2002-III, and Y.F. v. Turkey, no. 24209/94, § 33, ECHR 2003-IX). It can therefore embrace multiple aspects of the person's physical and social identity (see Mikulić v. Croatia, no. 53176/99, § 53, ECHR 2002-I). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (see, among other authorities, Benaddi v. the United Kingdom, no. 44599/98, § 47, ECHR 2001-I with further references, and Peck v. the United Kingdom, no. 44647/98, § 57, ECHR 2003-II). Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family (see, mutatis mutandis, Burghartz v. Switzerland, 22 February 1994, § 24, Series A no. 280-B, and Ünal Tekeli v. Turkey, no. 29865/96, § 42, ECHR 2004-X). Information about the person's health is an important element of private life (see Z v. Finland, 25 February 1997, § 71, Reports of Judgments and Decisions 1997-I). The Court furthermore considers that an individual's ethnic identity must be regarded as another such element (see, in particular, Article 6 of the Data Protection Convention quoted in paragraph 41 above, which lists personal data revealing racial origin as a special category of data along with other sensitive information about an individual). Article 8 protects, in addition, a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz, cited above, opinion of the Commission, p. 37, § 47, and Friedl v. Austria, 31 January 1995, Series A no. 305-B, opinion of the Commission, p. 20, § 45). The concept of private life moreover includes elements relating to a person's right to their image (see Sciacca v. Italy, no. 50774/99, § 29, ECHR 2005-IV) / 68. The Court notes at the outset that all three categories of the personal information retained by the authorities in the present case, namely fingerprints, DNA profiles and cellular samples, constitute personal data.
Leander v. Sweden	23/03/1987	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers	no violation of Article 8	Written personal data ; para 48. It is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1 (art. 8-1).
Rotaru v. Romania	04/05/2000	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers + ERASURE OR DESTRUCTION OF PERSONAL DATA	violation of Article 8 and 13	Personal data by professional life ; para 43. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life".
Z. v. Finland (no. 22009/93)	25/02/1997	DISCLOSURE OF PERSONAL DATA	violation of Article 8	Personal data by health data ; para 95. In this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art. 8). Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.
Bernh Larsen Holding As and Others v. Norway	14/03/2013	ELECTRONIC DATA	no violation of Article 8	Legal person ; para 80. The applicant companies complained that their right to respect for privacy, home and correspondence under Article 8 of the Convention had been infringed as a result of the Supreme Court's judgment of 20 November 2007 upholding the Directorate of Taxation's decision of 1 June 2004. // Personal data by tax information ; electronic data; para 3. The applicant companies complained under Article 8 of the Convention about a demand by the tax authorities that they make available for inspection at the tax office a backup copy of a computer server used jointly by the companies, in the context of a tax audit.
Uzun v. Germany	02/09/2010	GPS (Global Positioning System)	no violation of Article 8	Personal data by other elements ; 43-48. Personal data by indirect information related to an object; 41. In the applicant's view, his total surveillance via GPS had interfered with his right to respect for his private life. Even though the GPS receiver had been built into an object (S's car), it had been used to observe his (and S's) movements. It had enabled the investigating authorities to draw up a comprehensive pattern of his movements in public for months, by means of a measure which was very precise and difficult to detect. All his movements had been made known to third persons without his consent. The information gathered by the GPS surveillance had enabled the authorities to initiate further investigations. <i>Inter alia</i> , at the places he had travelled to.
Klass and Others v. Germany	06/09/1978	MASS SURVEILLANCE	no violation of Article 8	Personal data by telephone conversation ; para 41. Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision.
Liberty and Others v. the United Kingdom	01/07/2008	MASS SURVEILLANCE	violation of Article 8	Legal person ; para 1. The case originated in an application (no. 58243/00) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by Liberty, British Irish Rights Watch and the Irish Council for Civil Liberties, a British and two Irish civil liberties' organisations based in London and Dublin respectively, on 9 September 1999.
Godelli v. Italy	25/09/2012	ACCESS TO PERSONAL DATA	violation of Article 8	Personal data is related to a person identified or identifiable ; 58. In the present case the Court notes that where the birth mother has decided to remain anonymous, Italian law does not allow a child who was not formally recognised at birth and was subsequently adopted to request either access to non-identifying information concerning his or her origins or the disclosure of the mother's identity.
Halford v. the United Kingdom	25/06/1997	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8 and 13	Personal data by telephone conversation ; paras. 42 and 45. The applicant argued, and the Commission agreed, that the calls made on the telephones in Ms Halford's office at Merseyside police headquarters fell within the scope of "private life" and "correspondence" in Article 8 para. 1 (art. 8-1), since the Court in its case-law had adopted a broad construction of these expressions (see, for example, the Klass and Others v. Germany judgment of 6 September 1978, Series A no. 28, p. 21, para. 41; the Hüüg v. France judgment of 24 April 1990, Series A no. 176-B, p. 41, para. 8, and p. 52, para. 25; the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B; and the A. v. France judgment of 23 November 1993, Series A no. 277-B). There is no evidence of any warning having been given to Ms Halford, as a user of the internal telecommunications system operated at the Merseyside police headquarters, that calls made on that system would be liable to interception. She would, the Court considers, have had a reasonable expectation of privacy for such calls, which expectation was moreover reinforced by a number of factors. As Assistant Chief Constable she had sole use of her office where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the assurance, in response to a memorandum, that she could use her office telephones for the purposes of her sex-discrimination case.
Niemietz v. Germany	16/12/1992	CORRESPONDENCE. INFORMATION CONCERNING PROFESSIONAL ACTIVITIES	violation of Article 10	Personal data by professional life ; 6. Mr Niemietz alleged that the search of his law office had given rise to a breach of Article 8 (art. 8) of the Convention, (...) This submission was accepted by the Commission, on the basis that the search constituted an unjustified interference with the applicant's private life and home.
P.G. and J.H. v. the United Kingdom	25/09/2001	COLLECTION ON PERSONAL DATA: Voice samples	violation of Article 8, no violation of Article 8	Personal data by voice recording ; para. 34 and 37-34. The applicants complained that covert listening devices were used by the police to monitor and record their conversations at a flat, that information was obtained by the police concerning the use of a telephone at the flat and that listening devices were used while they were at the police station to obtain voice samples. The Court notes that it is not disputed that the surveillance carried out by the police at B's flat amounted to an interference with the right of the applicants to respect for their private life.
Sciacca v. Italy	11/01/2005	PHOTOS	violation of Article 8	Personal data by photos ; para. 29. Regarding whether there has been an interference, the Court reiterates that the concept of private life includes elements relating to a person's right to their image and that the publication of a photograph falls within the scope of private life (see Von Hannover, cited above, §§ 50-53). It has also given guidelines regarding the scope of private life and found that there is "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'".
Von Hannover v. Germany	07/02/2012	PHOTOS	No violation of Article 8	Personal data by photos, also in public context ; para. 95. The Court reiterates that the concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life. Publication of a photo may thus intrude upon a person's private life even where that person is a public figure (see Schiessel v. Austria (dec.), no. 62409/98, 21 February 2002; Von Hannover v. Germany, no. 59320/00, §§ 50 and 53, ECHR 2004-VI; Sciacca, cited above, § 29; and Petrina v. Romania, no. 78060/01, § 27, 14 October 2008).
Wisse v. France	20/12/2005	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	Personal data by sound ; 77. Dans sa jurisprudence, elle a souvent constaté que l'interception secrète de conversations ou d'images par le biais d'appareils d'enregistrement audio et vidéo entraînait dans le champ d'application de l'article 8 de la Convention pour ce qui est tant du droit au respect de la vie privée que de la correspondance.
Silver and Others v. the United Kingdom	25/03/1983	CORRESPONDENCE	violation of Article 8, 13 and 6, no violation of article 10	Personal data by correspondence ; 31. In the applicants' submission, the stopping or delaying of the 64 letters in question constituted a violation of Article 8 (art. 8) 8) 84. It is clear – and indeed this was not disputed – that there were "interferences by a public authority" with the exercise of the applicants' right to respect for their correspondence, which is guaranteed by paragraph 1 of Article 8 (art. 8-1).
Malone v. the United Kingdom	02/08/1984	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	Personal data by interception of communications ; 89. There has accordingly been a breach of Article 8 (art. 8) in the applicant's case as regards both interception of communications and release of records of metering to the police.
Gaskin v. the United Kingdom	07/07/1989	ACCESS TO PERSONAL DATA	violation of Article 8	Personal data by identity and origin ; 49. In the Court's opinion, persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development (...) Accordingly, the procedures followed failed to secure respect for Mr Gaskin's private and family life as required by Article 8 (art. 8) of the Convention. There has therefore been a breach of that provision.
Kruslin v. France	24/04/1990	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	Personal data by interception of communications ; 33. Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.

Anexo 5. La Jurisprudencia del TEDH en materia de protección de datos: principios en el tratamiento del derecho por parte del Tribunal				
Klass and Others v. Germany	06/09/1978	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	no violation of Article 8	Principio de fin legítimo. para 46. The Court, sharing the view of the Government and the Commission, finds that the aim of the G 10 is indeed to safeguard national security and/or to prevent disorder or crime in pursuance of Article 8 para 2 (art. 8-2).
Malone v. the United Kingdom	02/08/1984	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	Principio de ley, accesible y previsible. para. 66 y 67-66. The Court held in its Silver and Others judgment of 25 March 1983 (Series A no. 61, pp. 32-33, para. 85) that, at least as far as interferences with prisoners' correspondence were concerned, the expression "in accordance with the law" (prevue par la loi" in paragraph 2 of Article 8 (art. 8-2)) should be interpreted in the light of the same general principles as were stated in the Sunday Times judgment of 26 April 1979 (Series A no. 30) to apply to the comparable expression "prescribed by law" (prevue par la loi" in paragraph 2 of Article 10 (art. 10-2)). The first such principle was that the word "law/loi" is to be interpreted as covering not only written law but also unwritten law (see the above-mentioned Sunday Times judgment, p. 30, para. 47). A second principle, recognised by Commission, Government and applicant as being applicable in the present case, was that "the interference in question must have some basis in domestic law" (see the above-mentioned Silver and Others judgment, p. 33, para. 86). The expressions in question were, however, also taken to include requirements over and above compliance with the domestic law. Two of these requirements were explained in the following terms: "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail." (Sunday Times judgment, p. 31, para. 49; Silver and Others judgment, p. 33, paras. 87 and 88, 67. In the Government's submission, these two requirements, which were identified by the Court in cases concerning the imposition of penalties or restrictions on the exercise by the individual of his right to freedom of expression or to correspond, are less appropriate in the wholly different context of secret surveillance of communications. In the latter context, where the relevant law imposes no restrictions or controls on the individual to which he is obliged to conform, the paramount consideration would appear to the Government to be the lawfulness of the administrative action under domestic law. The Court would reiterate its opinion that the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention (see, mutatis mutandis, the above-mentioned Silver and Others judgment, p. 34, para. 90, and the Golder judgment of 21 February 1975, Series A no. 18, p. 17, para. 34). The phrase thus implies - and this follows from the object and purpose of Article 8 (art. 8) - that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 (art. 8-1) (see the report of the Commission, paragraph 121). Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident (see the above-mentioned Klass and Others judgment, Series A no. 28, pp. 21 and 23, paras. 42 and 49). Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.
Amann v. Switzerland	16/02/2000	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	Principio de ley, accesible y previsible. para. 50 y 56. The Court draws attention to its established case-law, according to which the expression "in accordance with the law" not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects (see the Kopp judgment cited above, p. 540, § 55). According to the Court's established case-law, a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual - if need be with appropriate advice - to regulate his conduct (see the Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, pp. 33-32, § 66). With regard to secret surveillance measures the Court has underlined the importance of that concept in the following terms (ibid., pp. 32-33, §§ 67-68):
Taylor-Sabori v. the United Kingdom	22/10/2002	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	Principio de ley. para 18 and 19. The Court notes that it is not disputed that the surveillance carried out by the police in the present case amounted to an interference with the applicant's rights under Article 8 § 1 of the Convention. It recalls that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of covert surveillance by public authorities, in this instance the police, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures (see Khan v. the United Kingdom, no. 35394/97, § 26, ECHR 2000-V). 15. At the time of the events in the present case there existed no statutory system to regulate the interception of paper messages transmitted via a private telecommunication system. It follows, as indeed the Government have accepted, that the interference was not "in accordance with the law".
Peck v. the United Kingdom	28/01/2003	COLLECTION ON PERSONAL DATA: Video surveillance + DISCLOSURE OF PERSONAL DATA	in breach of Article 8	Principio de fin legítimo. Para 85: In sum, the Court does not find that, in the circumstances of this case, there were relevant or sufficient reasons which would justify the direct disclosure by the Council to the public of stills from the footage in its own CCTV News article without the Council obtaining the applicant's consent or masking his identity, or which would justify its disclosures to the media without the Council taking steps to ensure so far as possible that such making would be effected by the media. The crime-prevention objective and context of the disclosures demanded particular scrutiny and care in these respects in the present case.
Shimovols v. Russia	21/06/2011	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	violation of Article 8	Principio de ley, accesible y previsible. para. 70. principio de constatar la injerencia para 64-66. For the above reasons, the Court does not consider that the domestic law indicates with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store in the Surveillance Database information on persons' private lives. In particular, it does not, as required by the Court's case-law, set out in a form accessible to the public any indication of the minimum safeguards against abuse. The interference with the applicant's rights under Article 8 was not, therefore, "in accordance with the law".
Kheili v. Switzerland	18/10/2011	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	violation of Article 8	Principio de necesidad. (sentencia no disponible). Al considerar que esta era una cuestión para la cual las autoridades debían demostrar la exactitud de los datos almacenados sobre la demandante, así como la gravedad de la injerencia en los derechos de dicha persona, el Tribunal dictaminó que la conservación de la palabra «prostituta» en el expediente policial no había sido necesaria en una sociedad democrática. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH. (disponible en European Handbook on Data Protection Law)
Leander v. Sweden	23/03/1987	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers	no violation of Article 8	Principios de necesidad y proporcionalidad. paras. 58, 59 y 67. The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued (see, inter alia, the Gillow judgment of 24 November 1986, Series A no. 109, p. 22, § 55). 59. However, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life. 67. The Court, like the Commission, thus reaches the conclusion that the safeguards contained in the Swedish personal control system meet the requirements of paragraph 2 of Article 8 (art. 8-2). Having regard to the wide margin of appreciation available to it, the respondent State was entitled to consider that in the present case the interests of national security prevailed over the individual interests of the applicant (see paragraph 59 above). The interference to which Mr. Leander was subjected cannot therefore be said to have been disproportionate to the legitimate aim pursued.
Rotaru v. Romania	04/05/2000	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers + ERASURE OR DESTRUCTION OF PERSONAL DATA	violation of Article 8 and 13	Principios de ley, accesible y previsible. para 57. The Court notes in this connection that section 8 of Law no. 14/1992 provides that information affecting national security may be gathered, recorded and archived in secret files. No provision of domestic law, however, lays down any limits on the exercise of those powers. Thus, for instance, the aforesaid Law does not define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed. Similarly, the Law does not lay down limits on the age of information held or the length of time for which it may be kept. Section 45 of the Law empowers the RIS to take over for storage and use the archives that belonged to the former intelligence services operating on Romanian territory and allows inspection of RIS documents with the Director's consent. The Court notes that this section contains no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained.
K.H. and Others v. Slovakia	28/06/2009	ACCESS TO PERSONAL DATA	violation of Article 8	Principio de establecimiento de confianza. 47. Bearing in mind that the exercise of the right under Article 8 to respect for one's private and family life must be practical and effective (see, for example, <i>Philikaridou v. Cyprus</i> , no. 23890/02, § 64, ECHR 2007-... [extracts], with further reference), the Court takes the view that such positive obligations should extend, in particular in cases like the present one where personal data are concerned, to the making available to the data subject of copies of his or her data files.
Haralambie v. Romania	27/10/2009	ACCESS TO PERSONAL DATA	violation of Article 8	Principio de transparencia. Paras: 62 and 79. Dans les observations complémentaires soumises le 22 octobre 2008, faisant suite à celles du requérant dans lesquelles il indiquait que le 23 juin 2008, il avait pu consulter son fichier personnel pour la période de 1979 à 1989, le Gouvernement fait valoir que le droit du requérant d'accès à son fichier personnel a été respecté. 79. Or, il est évident que, tant le fait de conserver, après les avoir recueillis, de tels renseignements dans un fichier tenu par des agents de l'État, que l'intérêt du requérant d'avoir accès au contenu de ce fichier relèvent de la « vie privée » au sens de l'article 8 § 1 de la Convention (voir <i>Rotaru précité</i> § 44 et <i>Riad, précité</i> , § 34). En l'occurrence, il s'agit pour l'intéressé de se voir communiquer des informations le concernant et dont il ignorait de toute évidence la nature exacte aussi longtemps qu'il n'y avait pas accès. Dès lors, il convenait qu'il puisse prendre connaissance de ces données, le cas échéant de caractère personnel, voire intime, et dont le caractère éventuellement inexact pouvait risquer de porter atteinte à sa réputation (voir mutatis mutandis <i>Gunes c. France</i> , no. 32157/06, § 26, 20 novembre 2008). Cela d'autant plus qu'il ressort du préambule de la loi no 187/1999 que le but de ces fichiers était de terroriser la population de sorte qu'il était légitime, dans ces conditions, que le requérant ait pensé que les informations collectées pouvaient toucher aux aspects les plus intimes de sa vie privée. Dans ces conditions, la Cour estime que l'article 8 trouve à s'appliquer en l'espèce.
S. and Marper v. the United Kingdom	04/12/2008	ELECTRONIC DATA	violation of Article 8	Principio de conservación limitada. para. 77 and 86. In view of the foregoing, the Court concludes that the retention of both cellular samples and DNA profiles discloses an interference with the applicants' right to respect for their private lives, within the meaning of Article 8 § 1 of the Convention. 86 (...) the retention of fingerprints constitutes an interference with the right to respect for private life.
Iordachi and Others v. Moldova	10/02/2009	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8 no violation of article 13	Principio de ley, accesible y previsible. para. 50. As regards the interception of communications of persons suspected of offences, the Court observes that in <i>Kopp</i> [cited above, § 74] it found a violation of Article 8 because the person empowered under Swiss secret surveillance law to draw a distinction between matters connected with a lawyer's work and other matters was an official of the Post Office's legal department. In the present case, while the Moldovan legislation, like the Swiss legislation, guarantees the secrecy of lawyer-client communications (see paragraph 18 above), it does not provide for any procedure which would give substance to the above provision. The Court is struck by the absence of clear rules defining what should happen other, for example, a phone call made by a client to his lawyer is intercepted.
Kopp v. Switzerland	25/03/1998	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	Principio de ley, accesible y previsible. para. 55. The expression "in accordance with the law", within the meaning of Article 8 § 2, requires firstly that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law.
Silver and Others v. the United Kingdom	25/03/1983	CORRESPONDENCE	violation of Article 8, 13 and 6, no violation of article 10	Principio de ley, accesible y previsible. para. 88. A third principle is that "a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail" (ibid.).
Taylor-Sabori v. the United Kingdom	22/10/2002	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	Principio de ley, accesible y previsible. para 18: It recalls that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of covert surveillance by public authorities, in this instance the police, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures (see Khan v. the United Kingdom, no. 35394/97, § 26, ECHR 2000-V).
The Sunday Times v. the United Kingdom	26/04/1979	FREEDOM OF PRESS	violation of Article 10, no violation of article 14	Principio de necesidad. para. 59. The Court has already had the occasion in its above-mentioned Handyside judgment to state its understanding of the phrase "necessary in a democratic society", the nature of its functions in the examination of issues turning on that phrase and the manner in which it will perform those functions.

Anexo 6. La Jurisprudencia del TEDH en materia de protección de datos: derechos en conflicto con el derecho a la protección de datos personales				
Mosley v. the United Kingdom	10/05/2011	INTERNET	no violation of Article 8	Ponderación de derechos: libertad de expresión-privacidad , paras 129 y 130. 129. Although punitive fines or criminal sanctions could be effective in encouraging compliance with any pre-notification requirement, the Court considers that these would run the risk of being incompatible with the requirements of Article 10 of the Convention. It reiterates in this regard the need to take particular care when examining restraints which might operate as a form of censorship prior to publication. It is satisfied that the threat of criminal sanctions or punitive fines would create a chilling effect which would be felt in the spheres of political reporting and investigative journalism, both of which attract a high level of protection under the Convention. 130. As noted above, the conduct of the newspaper in the applicant's case is open to severe criticism. Aside from publication of the articles detailing the applicant's sexual activities, the News of the World published photographs and video footage, obtained through clandestine recording, which undoubtedly had a far greater impact than the articles themselves. Despite the applicant's efforts in a number of jurisdictions, these images are still available on the Internet. The Court can see no possible additional contribution made by the audiovisual material (see paragraph 115 above), which appears to have been included in the News of the World's coverage merely to titillate the public and increase the embarrassment of the applicant.
Ashby Donald and Others v. France	10/01/2013	INTERNET	no violation of Article 10	Ponderación de derechos: privacidad y propiedad , 39 y 40. En l'espèce, les photographies litigieuses ont été publiées sur un site Internet appartenant à une société gérée par les deux premiers requérants, dans le but notamment de les vendre ou d'y donner accès contre rémunération. La démarche des requérants était donc avant tout commerciale. De plus, si l'on ne peut nier l'attrait du public pour la mode en général et les défilés de haute couture en particulier, on ne saurait dire que les requérants ont pris part à un débat d'intérêt général alors qu'ils se sont bornés à rendre des photographies de défilés de mode accessibles au public. 40. Ces considérations valent aussi dans le contexte de l'article 10 de la Convention, lorsque le but poursuivi par l'ingérence est la « protection » de droits d'autrui « au sens de cette disposition (voir MGN Limited c. Royaume-Uni, no 39401/04, § 142, 18 janvier 2011). Or, comme indiqué précédemment, l'ingérence dans le droit à la protection des données des requérants visait à la protection des droits d'auteur des créateurs de mode. Dès lors que l'article 1 du Protocole no 1 s'applique à la propriété intellectuelle, (Anheuser-Busch Inc. c. Portugal [GC], no 73049/01, § 72, CEDH 2007-I), elle visait ainsi à la protection de droits garantis par la Convention ou ses Protocoles.
SIA AKKA/LAA v. Latvia	12/07/2016	MUSICAL COPYRIGHT	no violation of Article 1 (protection of property) of Protocol No. 1 to the Convention and no violation of Article 6 § 1 (right to fair trial) of the Convention.	Ponderación de derechos: propiedad-privacidad , (sentencia no disponible) A fair balance between the requirements of the public interest (the interest of the broadcasting companies in obtaining a license that allowed them to legally spread the work, as well as the interest of the public to have access to the musical works), on the one hand, and the rights of the applicant organization to obtain equitable remuneration for the use of the musical work, on the other. Disponible en (press release issued by the Registrars of the Court, ECHR 251 (2016) 12.07.2016).
Axel Springer AG v. Germany	07/02/2012	FREEDOM OF PRESS	Violation of Article 10	Ponderación de derechos: pro libertad de expresión periodística , paras. 90 y 91 90. An initial essential criterion is the contribution made by photos or articles in the press to a debate of general interest (see Von Hannover, cited above, § 60; Leempoel & S.A. ED. Cné Revue v. Belgium, no. 64772/01, § 68, 9 November 2006; and Standard Verlags GmbH v. Austria (no. 2), no. 21277/05 § 46, 4 June 2009). The definition of what constitutes a subject of general interest will depend on the circumstances of the case. The Court nevertheless considers it useful to point out that it has recognised the existence of such an interest not only where the publication concerned political issues or crimes (see White v. Sweden, no. 42435/02, § 29, 19 September 2006; Egeland and Hænsel, cited above, § 58; and Leempoel & S.A. ED. Cné Revue, cited above, § 72), but also where it concerned sporting issues or performing artists (see Nikowitz and Verlagsgruppe News GmbH v. Austria, no. 5266/03, § 25, 22 February 2007; Colaço Mestre and SIC – Sociedade Independente de Comunicação, S.A. v. Portugal, nos. 11182/03 and 11319/03, § 28, 26 April 2007; and Sapan v. Turkey, no. 44102/04, § 34, 8 June 2010). However, the rumoured marital difficulties of a president of the Republic or the financial difficulties of a famous singer were not deemed to be matters of general interest (see Standard Verlags GmbH, cited above, § 52, and Hachette Filipacchi Associés (ICI PARIS), cited above, § 43). 91. The role or function of the person concerned and the nature of the activities that are the subject of the report and/or the publication constitute another important criterion, according to the preceding one. In that connection a distinction has to be made between private individuals and persons acting in a public context, as political figures or public figures. Accordingly, whilst a private individual unknown to the public may claim particular protection of his or her right to private life, the same is not true of public figures (see Minelli v. Switzerland (dec.), no. 14991/02, 14 June 2005, and Petrenco, cited above, § 55). A fundamental distinction needs to be made between reporting facts capable of contributing to a debate in a democratic society, relating to politicians in the exercise of their official functions for example, and reporting details of the private life of an individual who does not exercise such functions (see Von Hannover, cited above, § 63, and Standard Verlags GmbH, cited above, § 47). Whilst in the former case the press exercises its role of “public watchdog” in a democracy by imparting information and ideas on matters of public interest, that role appears less important in the latter case. Similarly, although in certain special circumstances the public's right to be informed can even extend to aspects of the private life of public figures, particularly where politicians are concerned, this will not be the case – even where the persons concerned are quite well known to the public – where the published photos and accompanying commentaries relate exclusively to details of the person's private life and have the sole aim of satisfying the curiosity of a particular readership in that respect (see Von Hannover, cited above, § 65 with the references cited therein, and Standard Verlags GmbH, cited above, § 53; see also point 8 of the Resolution of the Parliamentary Assembly – paragraph 51 above). In the latter case, freedom of expression calls for a narrower interpretation (see Von Hannover, cited above, § 66; Hachette Filipacchi Associés (ICI PARIS), cited above, § 40; and MGN Limited, cited above, § 143).
Birik v. Lithuania	25/11/2008	DISCLOSURE OF PERSONAL DATA	violation of Article 8	Ponderación de derechos: libertad de expresión-privacidad , para. 38. The protection of private life has to be balanced, among other things, against the freedom of expression guaranteed by Article 10 of the Convention. In that context the Court emphasises the duty of the press to impart information and ideas on matters of public interest (see, among many authorities, Observer and Guardian v. the United Kingdom, judgment of 26 November 1991, Series A no. 216, pp. 29-30, § 59). However, the Court notes that a fundamental distinction needs to be made between reporting facts – even if controversial – capable of contributing to a debate in a democratic society and making tawdry allegations about an individual's private life (see, mutatis mutandis, Von Hannover v. Germany, cited above § 63). As to respect for the individual's private life, the Court reiterates the fundamental importance of its protection in order to ensure the development of every human being's personality. That protection extends beyond the private family circle to include a social dimension. The Court considers that anyone, even if they are known to the general public, may legitimately expect the protection of and respect for their private life (ibid., § 69).
Müller and Others v. Switzerland	24/05/1998	FREEDOM OF ARTS	no violation of Article 10	Libertad de las artes bajo el art. 10 , Para. 27. The applicants indisputably exercised their right to freedom of expression – the first applicant by painting and then exhibiting the works in question, and the nine others by giving him the opportunity to show them in public at the “Fri-Art 81” exhibition they had mounted. Admittedly, Article 10 (art. 10) does not specify that freedom of artistic expression, in issue here, comes within its ambit; but neither, on the other hand, does it distinguish between the various forms of expression. As those appearing before the Court all acknowledged, it includes freedom of artistic expression – notably within freedom to receive and impart information and ideas – which affords the opportunity to take part in the public exchange of cultural, political and social information and ideas of all kinds.
Társaság a Szabadságjogokért v. Hungary	14/04/2009	ACCES TO INFORMATION	Violation of Article 10	Ponderación de derechos: libertad de expresión (recibir)-privacidad , paras. 27, 36-38. In view of the interest protected by Article 10, the law cannot allow arbitrary restrictions which may become a form of indirect censorship should the authorities create obstacles to the gathering of information. For example, the latter activity is an essential preparatory step in journalism and is an inherent, protected part of press freedom (see Dammann v. Switzerland (no. 77531/01, § 52, 25 April 2006). The function of the press includes the creation of forums for public debate. However, the realisation of this function is not limited to the media or professional journalists. In the present case, the preparation of the forum of public debate was conducted by a non-governmental organisation. The purpose of the applicant's activities can therefore be said to have been an essential element of informed public debate. The Court has repeatedly recognised civil society's important contribution to the discussion of public affairs (see, for example, Steel and Morris v. the United Kingdom (no. 68416/01, § 89, ECHR 2005-II). The applicant is an association involved in human rights litigation with various objectives, including the protection of freedom of information. It may therefore be characterised, like the press, as a social “watchdog”. In these circumstances, the Court is satisfied that its activities warrant similar constitutional protection to that afforded to the press. 36. In any event, the Court notes that “the right to freedom to receive information basically prohibits a Government from restricting a person from receiving information that others wish or may be willing to impart to him” (Leander, op. cit., § 74). It considers that the present case essentially concerns an interference – by virtue of the censorial power of an information monopoly – with the exercise of the functions of a social watchdog, like the press, rather than a denial of a general right of access to official documents. In this connection, a comparison can be drawn with the Court's previous concerns that preliminary obstacles created by the authorities in the way of press functions call for the most careful scrutiny (see Chauvy and Others v. France, no. 64915/01, § 66, ECHR 2004-VI). Moreover, the State's obligations in matters of freedom of the press include the elimination of barriers to the exercise of press functions; where, in issues of public interest, such barriers exist solely because of an information monopoly held by the authorities. The Court notes at this juncture that the information sought by the applicant in the present case was ready and available (see, a contrario, Guerra and Others v. Italy, 19 February 1998, § 53 in fine, Reports of judgments and Decisions 1998-I) and did not require the collection of any data by the Government. Therefore, the Court considers that the State had an obligation not to impede the flow of information sought by the applicant. 37. The Court observes that the applicant had requested information about the constitutional complaint eventually without the personal data of its author. Moreover, the Court finds it quite implausible that any reference to the private life of the MP, hence to a protected private sphere, could be discerned from his constitutional complaint. It is true that he had informed the press that he had lodged the complaint, and therefore his opinion on this public matter could, in principle, be identified with his person. However, the Court considers that it would be fatal for freedom of expression in the sphere of politics if public figures could censor the press and public debate in the name of their personality rights, alleging that their opinions on public matters are related to their person and therefore constitute private data which cannot be disclosed without consent. These considerations cannot justify, in the Court's view, the interference of which complaint is made in the present case. 38. The Court considers that obstacles created in order to hinder access to information of public interest may discourage those working in the media or related fields from pursuing such matters. As a result, they may no longer be able to play their vital role as “public watchdogs” and their ability to provide accurate and reliable information may be adversely affected.
Vereinigung bildender Künstler v. Austria	25/01/2007	FREEDOM OF ARTS	Violation of Article 10	Ponderación de derechos pro libertad de las artes , paras. 26 y 34. (utilización de cabezas de personas famosas en posturas sexuales dibujadas). 26. The Court reiterates that freedom of expression, as secured in paragraph 1 of Article 10, constitutes one of the essential foundations of a democratic society, indeed one of the basic conditions for its progress and for the self-fulfilment of the individual. Subject to paragraph 2, it is applicable not only to “information” or “ideas” that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any section of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no “democratic society”. Those who create, perform, distribute or exhibit works of art contribute to the exchange of ideas and opinions which is essential for a democratic society. Hence the obligation on the State not to encroach unduly on their freedom of expression. Artists and those who promote their work are certainly not immune from the possibility of limitations as provided for in paragraph 2 of Article 10. Whoever exercises his freedom of expression undertakes, in accordance with the express terms of that paragraph, “duties and responsibilities”; their scope will depend on his situation and the means he uses (see Müller and Others v. Switzerland, judgment of 24 May 1988, Series A no. 133, p. 22, §§ 33-34, with further references). 34. In the present case, the Court considers that the painting could hardly be understood to address details of Mr Meischberger's private life, but rather related to Mr Meischberger's public standing as a politician from the FPÖ. The Court notes that in this capacity Mr Meischberger has to display a wider tolerance in respect of criticism (see Ingens v. Austria, judgment of 8 July 1986, Series A no. 103, p. 26, § 42). The Court does not find unreasonable the view taken by the court of first instance that the scene in which Mr Meischberger was portrayed could be understood to constitute some sort of counter-attack against the Austrian Freedom Party, whose members had strongly criticised the painter's work.
Von Hannover v. Germany	07/02/2012	PHOTOS	no violation of Article 8	Ponderación de derechos: libertad de expresión-privacidad , paras. 118 y 124. 118. The Court observes that the fact that the Federal Court of Justice assessed the information value of the photo in question in the light of the accompanying article cannot be criticised under the Convention (see, mutatis mutandis, Tønsberg Bild A.S. and Hauken v. Norway, no. 510/04, § 87, 1 March 2007, and Österreichischer Rundfunk v. Austria, no. 35841/02, §§ 68-69, 7 December 2006). Regarding the characterisation of Prince Rainier's illness as an event of contemporary society, the Court is of the opinion that, having regard to the reasons advanced by the German courts, that interpretation cannot be considered unreasonable (see, mutatis mutandis, Editions Plon, cited above, §§ 46-57). It is worth mentioning in this connection that the Federal Court of Justice upheld the injunction forbidding publication of two other photographs showing the applicants in similar circumstances, precisely on the grounds that they were being published for entertainment purposes alone (see paragraphs 36-37 above). The Court can therefore accept that the photos in question, considered in the light of the accompanying articles, did contribute, at least to some degree, to a debate of general interest. It will therefore reiterate, on this point, that not only does the press have the task of imparting information and ideas on all matters of public interest, the public also has a right to receive them. 124. The Court observes that, in accordance with their case-law, the national courts carefully balanced the right of the publishing companies to freedom of expression against the right of the applicants to respect for their private life. In doing so, they attached fundamental importance to the question whether the photos, considered in the light of the accompanying articles, had contributed to a debate of general interest. They also examined the circumstances in which the photos had been taken.

Anexo 7. La Jurisprudencia del TEDH en materia de protección de datos: acciones de las personas

Leander v. Sweden	23/03/1987	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers	no violation of Article 8	<u>Rectification or erasure</u> : para 48. It is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1 (art. 8-1).
Rotaru v. Romania	04/05/2000	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers + ERASURE OR DESTRUCTION OF PERSONAL DATA	violation of Article 8 and 13	<u>Rectification or erasure</u> : para 46. The Court points out that both the storing by a public authority of information relating to an individual's private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8 § 1 of the Convention (see the following judgments: Leander cited above, p. 22, § 48; Kopp v. Switzerland, 25 March 1998, Reports 1998-II, p. 540, § 53; and Amann cited above, §§ 69 and 80).
Gaskin v. the United Kingdom	07/07/1989	ACCESS TO PERSONAL DATA	violation of Article 8	<u>Acces</u> : para. 41 and 49 (...) The Court will therefore examine whether the United Kingdom, in handling the applicant's requests for access to his case records, was in breach of a positive obligation flowing from Article 8 (art. 8) of the Convention. 49. In the Court's opinion, persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development.
Odièvre v. France	13/02/2003	ACCESS TO PERSONAL DATA	no violation of Article 8	<u>Acces</u> : para 24 and 28. The applicant complained that she was unable to obtain identifying information about her natural family and had thereby been prevented from finding out her personal history. She alleged a violation of Article 8 of the Convention. 28. In the instant case, the Court notes that the applicant's purpose is not to call into question her relationship with her adoptive parents but to discover the circumstances in which she was born and abandoned, including the identity of her natural parents and brothers. For that reason, it considers it necessary to examine the case from the perspective of private life, not family life, since the applicant's claim to be entitled, in the name of biological truth, to know her personal history is based on her inability to gain access to information about her origins and related identifying data.
K.H. and Others v. Slovakia	28/06/2009	ACCESS TO PERSONAL DATA	violation of Article 8	<u>Access</u> : paras. 44, 46, 47. The complaint in issue concerns the exercise by the applicants of their right of effective access to information concerning their health and reproductive status. As such it is linked to their private and family lives within the meaning of Article 8 (see, mutatis mutandis, Roche v. the United Kingdom [GC], no. 32555/96, § 155, ECHR 2005-X, with further reference). 46. The existence of such a positive obligation was established by the Court, among other circumstances, where applicants sought access to information about risks to one's health and well-being resulting from environmental pollution (Guerra and Others v. Italy, 19 February 1998, § 60, Reports 1998-I), information which would permit them to assess any risk resulting from their participation in nuclear tests (McGinley and Egan v. the United Kingdom, 9 June 1998, § 101, Reports of Judgments and Decisions 1998-III) or tests involving exposure to toxic chemicals (Roche v. the United Kingdom [GC], referred to above). The Court held, in particular, that a positive obligation arose to provide an "effective and accessible procedure" enabling the applicants to have access to "all relevant and appropriate information" (see, for example, Roche v. the United Kingdom [GC] cited above, § 162, with further references). Similarly, such a positive obligation was found to exist where applicants sought access to information to social service records containing information about their childhood and personal history (see Gaskin v. the United Kingdom, cited above and M.G. v. the United Kingdom, no. 39393/98, § 31, 24 September 2002). 47. Bearing in mind that the exercise of the right under Article 8 to respect for one's private and family life must be practical and effective (see, for example, Phinikaridou v. Cyprus, no. 23890/02, § 64, ECHR 2007-... (extracts), with further reference), the Court takes the view that such positive obligations should extend, in particular in cases like the present one where personal data are concerned, to the making available to the data subject of copies of his or her data files.
Cemalettin Canlı v. Turkey	18/11/2008	CORRESPONDENCE	violation of Article 8	<u>Rectification or erasure</u> : paras. 18. (and 33, 43, 44). 18. The applicant complained that the records kept arbitrarily and unlawfully by the police and the publication in the national press of the details of those records had had adverse effects on his private life within the meaning of Article 8 of the Convention
Segerstedt-Wiberg and Others v. Sweden	06/06/2006	ACCESS TO PERSONAL DATA	no violation of Article 8	<u>Rectification or erasure</u> : para 89 y 90.89. In so far as the first applicant is concerned, the Court finds no reason to doubt that the reasons for keeping on record the information relating to bomb threats in 1990 against her and certain other personalities were relevant and sufficient as regards the aim of preventing disorder or crime. The measure was at least in part motivated by the interest in protecting her security; there can be no question of any disproportionate interference with her right to respect for private life thus being entailed. The Court has received no particulars about the precise contents of the documents released to the applicant on 13 December 2002 and will not therefore examine that matter. 90. However, as to the information released to the second applicant (namely, his participation in a political meeting in Warsaw in 1967), the Court, bearing in mind the nature and age of the information, does not find that its continued storage is supported by reasons which are relevant and sufficient as regards the protection of national security. Similarly, the storage of the information released to the fifth applicant could for the most part hardly be deemed to correspond to any actual relevant national security interests for the respondent State. The continued storage of the information to the effect that he, in 1969, had allegedly advocated violent resistance to police control during demonstrations was supported by reasons that, although relevant, could not be deemed sufficient thirty years later. Therefore, the Court finds that the continued storage of the information released to the second and fifth applicants entailed a disproportionate interference with their right to respect for private life.
Ciubotaru v. Moldova,	27/10/2010	IDENTITY	violation of Article 8	<u>Rectification or erasure</u> : paras 51 y 59. 51. The Court reiterates that in the assessment of the present case it should be borne in mind that the Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective (see Airey v. Ireland, 9 October 1979, § 24, Series A no. 32). Whilst Article 8 contains no explicit procedural requirements, it is important for the effective enjoyment of the rights guaranteed by this provision that the relevant decision-making process is fair and such as to afford due respect to the interests safeguarded by it. Such a process may require the existence of an effective procedural framework whereby an applicant can assert his or her rights under Article 8 under conditions of fairness, including as regards matters of proof and evidence. The Court recalls in this latter connection that in the case of I. v. Finland (no. 20511/03, § 44, 17 July 2008) in finding a violation of Article 8 of the Convention the Court gave weight to the fact that the State had placed too heavy a burden of proof on the applicant in civil proceedings in which she sought compensation for the dissemination of information about her medical condition. 59. Having regard to the circumstances of the case as a whole, it cannot be said that the procedure in place to enable the applicant to have his recorded ethnicity changed complied with Moldova's positive obligations to safeguard his right to respect for his private life. For the Court, the State's failure consists in the inability for the applicant to have examined his claim to belong to a certain ethnic group in the light of the objectively verifiable evidence adduced in support of that claim. The Court therefore concludes that the authorities failed to comply with their positive obligation to secure to the applicant the effective respect for his private life.
M.S. v. Sweden (no. 20837/92)	27/02/1997	DISCLOSURE OF PERSONAL DATA	no violation of Article 8	<u>The right to object due to the data subject's particular situation</u> : para.33. With reference to the arguments set out in paragraph 31 above, the Government disputed that the communication of the data in question amounted to an interference with the applicant's right to respect for her private life under Article 8. 34. The applicant and the Commission, stressing that information of a private and sensitive nature had been disclosed without her consent to a certain number of people at the Office, maintained that the measure constituted an interference. 35. The Court notes that the medical records in question contained highly personal and sensitive data about the applicant, including information relating to an abortion. Although the records remained confidential, they had been disclosed to another public authority and therefore to a wider circle of public servants (see paragraphs 12–13 above). Moreover, whilst the information had been collected and stored at the clinic in connection with medical treatment, its subsequent communication had served a different purpose, namely to enable the Office to examine her compensation claim. It did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office (see paragraph 10 above). Having regard to these considerations, the Court finds that the disclosure of the data by the clinic to the Office entailed an interference with the applicant's right to respect for private life guaranteed by paragraph 1 of Article 8.
Mosley v. the United Kingdom	10/05/2011	INTERNET	no violation of Article 8	<u>The right to object due to the data subject's particular situation</u> : para. 65 and 66. 65. The applicant complained that the United Kingdom had violated its positive obligations under Article 8 of the Convention, taken alone and taken together with Article 13, by failing to impose a legal duty on the News of the World to notify him in advance in order to allow him the opportunity to seek an interim injunction and thus prevent publication of material which violated his right to respect for his private life. The Government contested that argument. 66. In the Court's view, the complaint under Article 13 as to the absence of an effective domestic remedy is a reformulation of the applicant's complaint under Article 8 of the Convention that the respondent State did not ensure respect for the applicant's private life, and is subsidiary to it (see Armonienė v. Lithuania, no. 36919/02, § 23, 25 November 2008; and Birlik v. Lithuania, no. 23373/03, § 23, 25 November 2008).

Anexo 8. La Jurisprudencia del TEDH en materia de protección de datos: obligaciones de los Estados

Gaskin v. the United Kingdom	07/07/1989	ACCESS TO PERSONAL DATA	violation of Article 8	<u>Fair balance between interests for the existence of positive obligations</u>: para. 42. In accordance with its established case-law, the Court, in determining whether or not such a positive obligation exists, will have regard to the "fair balance that has to be struck between the general interest of the community and the interests of the individual ... In striking this balance the aims mentioned in the second paragraph of Article 8 (art. 8) may be of a certain relevance, although this provision refers in terms only to 'interferences' with the right protected by the first paragraph - in other words is concerned with the negative obligations flowing therefrom ..." (see the Rees judgment of 17 October 1986, Series A no. 106, p. 15, para. 37). <u>Interests in state's margin of appreciation, not enough for the Court</u>: para. 44 and 49. In this respect, the balance struck by both the circular and the resolution between the interests of the individual seeking access to the records on the one hand and, on the other hand, the interests of those who have supplied information in confidence and the wider public interest in the maintenance of full and candid records, was said by the Government to be proper, rational, reasonable and consistent with their obligations under Article 8 (art. 8). There was thus no failure on the part of the United Kingdom to secure the applicant's right to respect for private life guaranteed by that provision. 49. In the Court's opinion, persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development. On the other hand, it must be borne in mind that confidentiality of public records is of importance for receiving objective and reliable information, and that such confidentiality can also be necessary for the protection of third persons. Under the latter aspect, a system like the British one, which makes access to records dependent on the consent of the contributor, can in principle be considered to be compatible with the obligations under Article 8 (art. 8), taking into account the State's margin of appreciation. The Court considers, however, that under such a system the interests of the individual seeking access to records relating to his private and family life must be secured when a contributor to the records either is not available or improperly refuses consent. Such a system is only in conformity with the principle of proportionality if it provides that an independent authority finally decides whether access has to be granted in cases where a contributor fails to answer or withholds consent. No such procedure was available to the applicant in the present case.
Odièvre v. France	13/02/2003	ACCESS TO PERSONAL DATA	no violation of Article 8	<u>Existence of positive obligations, fair balance between interests in state's margin of appreciation</u>: para. 40. The Court reiterates that although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (see X and Y v. the Netherlands, judgment of 26 March 1985, Series A no. 91, p. 11, § 23). The boundaries between the State's positive and negative obligations under Article 8 do not lend themselves to precise definition. The applicable principles are nonetheless similar. In particular, in both instances regard must be had to the fair balance which has to be struck between the competing interests; and in both contexts the State enjoys a certain margin of appreciation (see Mikulić, cited above, § 58). <u>Margin of appreciation for States to decide measures which secure the Convention's rights</u>: para 46 and 47. The Court reiterates that the choice of the means calculated to secure compliance with Article 8 in the sphere of the relations of individuals between themselves is in principle a matter that falls within the Contracting States' margin of appreciation. In this connection, there are different ways of ensuring "respect for private life", and the nature of the State's obligation will depend on the particular aspect of private life that is at issue (see X and Y v. the Netherlands, cited above, p. 12, § 24). 47. (...) the Court concludes that States must be afforded a margin of appreciation to decide which measures are apt to ensure that the rights guaranteed by the Convention are secured to everyone within their jurisdiction.
K.U. v. Finland	02/12/2008	INTERNET	violation of Article 8	<u>Existence of positive obligation, even in the relationship of individuals, state's margin of appreciation</u>: 42. The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see Airey v. Ireland, 9 October 1979, § 32, Series A no. 32). 43. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is at issue. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions (see X and Y v. the Netherlands, cited above, §§ 23-24 and 27; August v. the United Kingdom (dec.), no. 36505/02, 21 January 2003; and M.C. v. Bulgaria, no. 39272/98, § 150, ECHR 2003-XII). <u>Fair balance between interests in state's margin of appreciation, not enough for the Court</u>: para. 46 and 49. (...) For the Court, States have a positive obligation inherent in Article 8 of the Convention to criminalise offences against the person, including attempted offences, and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution (see, mutatis mutandis, M.C. v. Bulgaria, cited above, § 153). Where the physical and moral welfare of a child is threatened, such injunction assumes even greater importance. The Court notes in this connection that sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private life. 49. The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality.
Köpke v. Germany	05/10/2010	VIDEO SURVEILLANCE	no violation of Article 8, inadmissible	<u>Existence of positive obligation, even in the relationship of individuals, state's margin of appreciation enough</u>: para. 2. The Court further reiterates that there are different ways of ensuring respect for private life and that the nature of the State's obligation will depend on the particular aspect of private life that is at issue. The choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation. The Court has found, however, that in certain circumstances, the State's positive obligation under Article 8 is only adequately complied with if the State safeguards respect for private life in the relations of individuals between themselves by legislative provisions providing a framework for reconciling the various interests which compete for protection in the relevant context. The Court has thus considered, in particular, that effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions (see X and Y v. the Netherlands, cited above, §§ 23, 24 and 27; M.C. v. Bulgaria, cited above, § 150, both concerning serious sexual offences against minors; and K.U. v. Finland, cited above, §§ 43, 49, concerning an advertisement of a sexual nature in the name of a minor on an Internet dating site). It has further held, for instance, that the Contracting Parties are obliged to set up an adequate regulatory framework in order to secure the respect of the physical integrity of hospital patients. In the present case, the Court therefore has to examine whether the State, in the context of its positive obligations under Article 8, has struck a fair balance between the applicant's right to respect for her private life and both her employer's interest in protection of its property rights, guaranteed by Article 1 of Protocol no. 1 to the Convention, and the public interest in the proper administration of justice. The Court further observes that this case-law has been expressly referred to and applied by the domestic courts in the applicant's case. Moreover, it takes the view that a covert video surveillance at the workplace following substantiated suspicions of theft does not concern a person's private life to an extent which is comparable to the affection of essential aspects of private life by grave acts in respect of which the Court has considered protection by legislative provisions indispensable (see above). In these circumstances, the Court is satisfied that, at least at the relevant time, respect for private life in the relations of the applicant and her employer in the context of a covert video surveillance could still adequately be protected by the domestic courts' case-law, without the State having been obliged to set up a legislative framework in order to comply with its positive obligation under Article 8.

K.H. and Others v. Slovakia	28/06/2009	ACCESS TO PERSONAL DATA	violation of Article 8	<u>Existence of positive obligations, some examples:</u> para.45, 46 and 47. The Court reiterates that, in addition to the primarily negative undertakings in Article 8 of the Convention, there may be positive obligations inherent in effective respect for one's private life. In determining whether or not such a positive obligation exists, it will have regard to the fair balance that has to be struck between the general interest of the community and the competing interests of the individual concerned, the aims in the second paragraph of Article 8 being of a certain relevance (see, for example, Gaskin v. the United Kingdom, 7 July 1989, § 42, Series A no. 160). 46. The existence of such a positive obligation was established by the Court, among other circumstances, where applicants sought access to information about risks to one's health and well-being resulting from environmental pollution (Guerra and Others v. Italy, 19 February 1998, § 60, Reports 1998-I), information which would permit them to assess any risk resulting from their participation in nuclear tests (McGinley and Egan v. the United Kingdom, 9 June 1998, § 101, Reports of Judgments and Decisions 1998-III) or tests involving exposure to toxic chemicals (Roche v. the United Kingdom [GC], referred to above). The Court held, in particular, that a positive obligation arose to provide an "effective and accessible procedure" enabling the applicants to have access to "all relevant and appropriate information" (see, for example, Roche v. the United Kingdom [GC] cited above, § 162, with further references). Similarly, such a positive obligation was found to exist where applicants sought access to information to social service records containing information about their childhood and personal history (see Gaskin v. the United Kingdom, cited above and M.G. v. the United Kingdom, no. 39393/98, § 31, 24 September 2002). 47. Bearing in mind that the exercise of the right under Article 8 to respect for one's private and family life must be practical and effective (see, for example, Phinikaridou v. Cyprus, no. 23890/02, § 64, ECHR 2007-... (extracts), with further reference), the Court takes the view that such positive obligations should extend, in particular in cases like the present one where personal data are concerned, to the making available to the data subject of copies of his or her data files. 58. There has therefore been a failure to fulfil the positive obligation to ensure effective respect for the applicants' private and family lives in breach of Article 8 of the Convention.
-----------------------------	------------	-------------------------	------------------------	---

Anexo 9. La Jurisprudencia del TEDH en materia de protección de datos: reconocimiento expreso de la protección de datos personales por parte el TEDH y su relación con el Convenio 108				
Leander v. Sweden	23/03/1987	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers	no violation of Article 8	<u>First antecedent of data protection (still within private life, not expressly mentioned):</u> para. 48. It is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1 (art. 8-1).
Gaskin v. the United Kingdom	07/07/1989	ACCESS TO PERSONAL DATA	violation of Article 8	<u>Second antecedent of data protection (still within private life, not expressly mentioned):</u> para. 37. The Court agrees with the Commission. The records contained in the file undoubtedly do relate to Mr Gaskin's "private and family life" in such a way that the question of his access thereto falls within the ambit of Article 8 (art. 8). This finding is reached without expressing any opinion on whether general rights of access to personal data and information may be derived from Article 8 para. 1 (art. 8-1) of the Convention. The Court is not called upon to decide in abstracto on questions of general principle in this field but rather has to deal with the concrete case of Mr Gaskin's application.
Z. v. Finland (no. 22009/93)	25/02/1997	DISCLOSURE OF PERSONAL DATA	violation of Article 8	<u>First mention of data protection within art. 8, and equation between guarantees of private life in art. 8 CEDH and protection of personal data in C108 :</u> para. 95. In this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art. 8). Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community (...)The domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (art. 8) (see, mutatis mutandis, Articles 3 para. 2 (c), 5, 6 and 9 of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series no. 108, Strasbourg, 1981).
M.S. v. Sweden (no. 20837/92)	27/02/1997	DISCLOSURE OF PERSONAL DATA	no violation of Article 8	<u>Importance of data protection for respect of private life art. 8 CEDH. :</u> para.41. The Court reiterates that the protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (see the Z v. Finland judgment of 25 February 1997, Reports of Judgments and Decisions 1997-I, p. 347, § 95)
Amann v. Switzerland	16/02/2000	COLLECTION ON PERSONAL DATA: Interception of communications, phone tapping and secret surveillance	violation of Article 8	<u>Private life = definition of personal data in C108:</u> para. 65. The Court reiterates that the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48). It points out in this connection that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42). That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2).
Rotaru v. Romania	04/05/2000	STORAGE AND USE OF PERSONAL DATA: Storage in secret registers + ERASURE OR DESTRUCTION OF PERSONAL DATA	violation of Article 8 and 13	<u>Consolidates jurisprudence. Private life= definition of personal data in C108. Protection of personal data is protected by art. 8 CEDH:</u> para. 43 and 44.43. The Court reiterates that the storing of information relating to an individual's private life in a secret register and the release of such information come within the scope of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48). Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings: furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford v. the United Kingdom judgment of 25 June 1997, Reports 1997-III, pp. 1015-16, §§ 42-46). The Court has already emphasised the correspondence of this broad interpretation with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined in Article 2 as "any information relating to an identified or identifiable individual" (see Amann v. Switzerland [GC], no. 27798/95, § 65, ECHR 2000-II). Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past. 44. In the instant case the Court notes that the RIS's letter of 19 December 1990 contained various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than fifty years earlier. In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life" for the purposes of Article 8 § 1 of the Convention. That is all the more so in the instant case as some of the information has been declared false and is likely to injure the applicant's reputation. Article 8 consequently applies.
S. and Marper v. the United Kingdom	04/12/2008	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	violation of Article 8	<u>Used as a relevant international material to take into consideration:</u> para 41. The Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data ("the Data Protection Convention"), which entered into force for the United Kingdom on 1 December 1987, defines "personal data" as any information relating to an identified or identifiable individual ("data subject"). The Convention provides, inter alia (...)
Bernh Larsen Holding As and Others v. Norway	14/03/2013	ELECTRONIC DATA	no violation of Article 8	<u>Used as a relevant international material to take into consideration:</u> para. 76. The Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data ("the Data Protection Convention"), which entered into force for the United Kingdom on 1 December 1987 (...)
Cemalettin Canli v. Turkey	18/11/2008	CORRESPONDENCE	violation of Article 8	<u>Private life = definition of protection of personal data in C108:</u> para. 34. The Court considers this interpretation of the notion of "private life" to be in line with the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined in Article 2 as "any information relating to an identified or identifiable individual" (paragraph 17 above).

Anexo 10. La Jurisprudencia del TEDH en materia de protección de datos: casos con mayor incidencia de las nuevas tecnologías					
CASO	FECHA	TEMÁTICA	DERECHOS EN CUESTIÓN	INCIDENCIA TIC	OBSERVACIONES DE LA CORTE
Uzun v. Germany	02/09/2010	COLLECTION ON PERSONAL DATA: GPS data + STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	no violation of Article 8	The applicant, suspected of involvement in bomb attacks by a left-wing extremist movement, complained in particular that his surveillance via GPS and the use of the data obtained thereby in the criminal proceedings against him had violated his right to respect for private life.	the Court noted, it had pursued the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime. It had also been proportionate: GPS surveillance had been ordered only after less intrusive methods of investigation had proved insufficient
Roman Zakharov v. Russia	04/12/2015	TELECOMMUNICATIONS	violation of Article 8	This case concerned the system of secret interception of mobile telephone communications in Russia. The applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law-enforcement agencies to carry out operational-search activities and that, without sufficient safeguards under Russian law, this permitted blanket interception of communications.	The Court held that there had been a violation of Article 8 of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications
Szabó and Vissy v. Hungary	12/01/2016	MASS SURVEILLANCE	violation of Article 8, no violation of Article 13	This case concerned Hungarian legislation on secret anti-terrorist surveillance introduced in 2011. The applicants complained in particular that they could potentially be subjected to unjustified and disproportionately intrusive measures within the Hungarian legal framework on secret surveillance for national security purposes (namely, "section 7/E (3) surveillance"). They notably alleged that this legal framework was prone to abuse, notably for want of judicial control.	In this case the Court held that there had been a violation of Article 8 of the Convention. It accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents. However, the Court was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. Notably, the scope of the measures could include virtually anyone in Hungary, with new technologies enabling the Government to intercept masses of data easily concerning even persons outside the original range of operation. Furthermore, the ordering of such measures was taking place entirely within the realm of the executive and without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place
Big Brother Watch and Others v. the United Kingdom PENDING	09/01/2014	MASS SURVEILLANCE	Article 8 (right to respect for private life) of the Convention.	The applicants, three NGOs and one academic working internationally in the fields of privacy and freedom of expression, allege they are likely to have been the subjects of surveillance by the United Kingdom intelligence services. Their concerns have been triggered by media coverage following the revelations by Edward Snowden, a former systems administrator with the United States National Security Agency (the NSA).	pending
Bureau of Investigative Journalism and Alice Ross v. the United Kingdom PENDING	05/01/2015	MASS SURVEILLANCE	Articles 8 (right to respect for private life) and 10 (freedom of expression) of the Convention.	his case concerns the allegations of the applicants – the Bureau of Investigative Journalism and an investigative reporter who has worked for the Bureau – regarding the interception of both internet and telephone communications by government agencies in the United Kingdom, and, in particular, by the Government Communication Headquarters (GCHQ), as revealed by Edward Snowden, a former systems administrator with the United States National Security Agency (the NSA). The applicants mainly complain that the blanket interception, storage and exploitation of communication amount to disproportionate interference with journalistic freedom of expression.	pending
S. and Marper v. the United Kingdom	04/12/2008	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	violation of Article 8	This case concerned the indefinite retention in a database of the applicants' fingerprints, cell samples and DNA profiles: after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in the other case.	It considered in particular that the use of modern scientific techniques in the criminal- justice system could not be allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. Any State claiming a pioneer role in the development of new technologies bore special responsibility for "striking the right balance".
B.B. v. France , Gardel v. France and M.B. v. France	17/12/2009	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	no violation of Article 8	The applicants in these cases, who had been sentenced to terms of imprisonment for rape of 15 year old minors by a person in a position of authority, complained in particular about their inclusion in the automated national judicial database of sex offenders (<i>Fichier judiciaire national automatisé des auteurs d'infractions sexuelles</i>).	The Court reaffirmed in particular that the protection of personal data was of fundamental importance to a person's enjoyment of respect for his or her private and family life, all the more so where such data underwent automatic processing, not least when such data were used for police purposes. However, the Court could not call into question the prevention-related objectives of the database.
Shimovolos v. Russia	21/06/2011	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	violation of Article 8	This case concerned the registration of a human rights activist in the so-called "surveillance database", which collected information about his movements, by train or air, within Russia, and his arrest.	Consequently, the Court found that the domestic law did not indicate with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store information on individuals' private lives in the database. In particular, it did not set out in a form accessible to the public any indication of the minimum safeguards against abuse.
Peruzzo and Martens v. Germany	04/06/2013	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	inadmissible	The applicants, who had been convicted of serious criminal offences, complained about the domestic courts' orders to collect cellular material from them and to store it in a database in the form of DNA profiles for the purpose of facilitating the investigation of possible future crimes.	The Court declared the application inadmissible as manifestly ill-founded. It found that the domestic rules on the taking and retention of DNA material from persons convicted of offences reaching a certain level of gravity as applied in the case of the applicants had struck a fair balance between the competing public and private interests and fell within the respondent State's acceptable margin of appreciation.
Dagregorio and Mosconi v. France	30/05/2017	STORAGE AND USE OF PERSONAL DATA: In the context of criminal justice	inadmissible	The applicants are two trade unionists who took part in the occupation and immobilisation of the <i>Société nationale Corse Méditerranée</i> (SNCM) ferry "Pascal Paoli" during the company takeover by a financial operator. The case concerned their refusal to undergo biological testing, the results of which were to be included in the national computerised DNA database (FNAEG). The applicants, having been convicted at first instance and on appeal, did not lodge an appeal on points of law.	The Court declared the application inadmissible for non-exhaustion of domestic remedies.
Breyer v. Germany PENDING	21/03/2016	STORAGE AND USE OF PERSONAL DATA: Telecommunication service providers' data	Articles 8 (right to respect for private life and correspondence) and 10 (freedom of expression)	The application concerns the legal obligation of telecommunication providers to store personal details of all their customers.	pending

Čalović v. Montenegro PENDING	31/03/2016	STORAGE AND USE OF PERSONAL DATA: Telecommunication service providers' data	Articles 8 (right to respect for private life), 34 (individual applications) and 35 (admissibility criteria) of the Convention.	The applicant complains about the powers of the police to access directly all data of the mobile telecommunication provider to which she is subscribed, therefore including her own, in an uncontrolled manner.	pending
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland	27/06/2017	DISCLOSURE OF PERSONAL DATA	no violation of Article 10	After two companies had published the personal tax information of 1.2 million people, the domestic authorities ruled that such wholesale publication of personal data had been unlawful under data protection laws, and barred such mass publications in future. The companies complained that the ban had violated their right to freedom of expression.	The Grand Chamber held, by fifteen votes to two, that there had been no violation of Article 10 (freedom of expression) of the Convention. It noted in particular that the ban had interfered with the companies' freedom of expression. However, it had not violated Article 10 because it had been in accordance with the law, it had pursued the legitimate aim of protecting individuals' privacy, and it had struck a fair balance between the right to privacy and the right to freedom of expression. In this case, the Grand Chamber agreed with the conclusion of the domestic courts, that the mass collection and wholesale dissemination of taxation data had not contributed to a debate of public interest, and had not been for a solely journalistic purpose.
Liberty and Others v. the United Kingdom	01/07/2008	MASS SURVEILLANCE	violation of Article 8	The applicants, a British and two Irish civil liberties' organisations, alleged that, between 1990 and 1997, their telephone, facsimile, e-mail and data communications, including legally privileged and confidential information, were intercepted by an Electronic Test Facility operated by the British Ministry of Defence. They had lodged complaints with the Interception of Communications Tribunal, the Director of Public Prosecutions and the Investigatory Powers Tribunal to challenge the lawfulness of the alleged interception of their communications, but to no avail.	It did not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the authorities to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material
Mandil v. France, Barreau and Others v. France and Deceuninck v. France	13/11/2011	ELECTRONIC DATA	inadmissible	The applicants were "Faucheurs volontaires" (Volunteer Reapers) who had participated in digging up experimental crops of transgenic beetroot. The applicant in the first case complained about his conviction for refusing to provide a biological sample to be stored on the national computerised DNA database; the applicants in the second case argued that the storage of their DNA on the national computerised database and the conviction of a number of them for refusing to provide a biological sample amounted to a violation of their right to respect for private life; the applicant in the third case submitted in particular that the order to take cell samples containing his genetic information constituted a disproportionate interference with his integrity and his private life.	The Court declared the applications inadmissible for failure to respect duty of confidentiality in friendly settlement negotiations. It considered that the applicants had violated the principle of confidentiality enshrined in Article 39 § 2 of the Convention and Rule 62 of the Rules of Court and that their conduct had constituted a violation of the right of individual petition for the purposes of Article 35 § 3 (a) of the Convention.